

SECTION 28 05 00
COMMON WORK RESULTS FOR ELECTRONIC SAFETY AND SECURITY

PART 1 - GENERAL

1.1 RELATED DOCUMENTS

- A. Drawings and general provisions of the Contract, including General and Supplementary Conditions and Division 1 Specification Sections, apply to this Section.

1.2 SUMMARY

- A. Section Includes:
 - 1. Electronic safety and security equipment coordination and installation.
 - 2. Sleeves for raceways and cables.
 - 3. Sleeve seals.
 - 4. Grout.
 - 5. Common electronic safety and security installation requirements.

1.3 DEFINITIONS

- A. EPDM: Ethylene-propylene-diene terpolymer rubber.
- B. NBR: Acrylonitrile-butadiene rubber.

1.4 SUBMITTALS

- A. Product Data: For sleeve seals.

1.5 COORDINATION

- A. Coordinate arrangement, mounting, and support of electronic safety and security equipment:
 - 1. To allow maximum possible headroom unless specific mounting heights that reduce headroom are indicated.
 - 2. To provide for ease of disconnecting the equipment with minimum interference to other installations.
 - 3. To allow right of way for piping and conduit installed at required slope.
 - 4. So connecting raceways, cables, wireways, cable trays, and busways will be clear of obstructions and of the working and access space of other equipment.
- B. Coordinate installation of required supporting devices and set sleeves in cast-in-place concrete, masonry walls, and other structural components as they are constructed.
- C. Coordinate location of access panels and doors for electronic safety and security items that are behind finished surfaces or otherwise concealed. Access doors and panels are specified in Division 8 Section "Access Doors and Frames."

- D. Coordinate sleeve selection and application with selection and application of firestopping specified in Division 7 Section "Firestopping."

1.6 RECORD DRAWINGS

- A. Contractor shall provide owner with a complete set of accurate Record Drawings for all work performed under this contract.
 - 1. Record Drawings shall include all approved change orders and pertinent RFI responses.
 - 2. Include actual dimensions of equipment furnished under this contractor where shown on the floor plans.
 - 3. Record Drawings shall include work performed by all sub-contractors retained.
 - 4. Record Drawings shall include the words "RECORD DRAWING" on each sheet.
- B. Submission:
 - 1. Submit one set of record Drawings for review by Engineer prior to submission of closeout documents. Record Drawings shall be submitted using the established submittal process.
 - 2. Upon satisfactory review of the Record Drawing submittals by Engineer, provide three (3) copies in electronic format with closeout documents
 - 3. Electronic Record Drawings shall include multi-sheet PDF files combined and named by discipline.

PART 2 - PRODUCTS

2.1 SLEEVES FOR RACEWAYS AND CABLES

- A. Steel Pipe Sleeves: ASTM A 53/A 53M, Type E, Grade B, Schedule 40, galvanized steel, plain ends.
- B. Sleeves for Rectangular Openings: Galvanized sheet steel.
 - 1. Minimum Metal Thickness:
 - a. For sleeve cross-section rectangle perimeter less than 50 inches and no side more than 16 inches, thickness shall be 0.052 inch.
 - b. For sleeve cross-section rectangle perimeter equal to, or more than, 50 inches and 1 or more sides equal to, or more than, 16 inches, thickness shall be 0.138 inch.

2.2 SLEEVE SEALS

- A. Description: Modular sealing device, designed for field assembly, to fill annular space between sleeve and raceway or cable.
 - 1. Manufacturers: Subject to compliance with requirements, available manufacturers offering products that may be incorporated into the Work include, but are not limited to, the following:
 - a. Advance Products & Systems, Inc.
 - b. Calpico, Inc.

- c. Metraflex Co.
 - d. Pipeline Seal and Insulator, Inc.
- 2. Sealing Elements: EPDM interlocking links shaped to fit surface of cable or conduit. Include type and number required for material and size of raceway or cable.
 - 3. Pressure Plates: Carbon steel. Include two for each sealing element.
 - 4. Connecting Bolts and Nuts: Carbon steel with corrosion-resistant coating of length required to secure pressure plates to sealing elements. Include one for each sealing element.

2.3 GROUT

- A. Nonmetallic, Shrinkage-Resistant Grout: ASTM C 1107, factory-packaged, nonmetallic aggregate grout, noncorrosive, nonstaining, mixed with water to consistency suitable for application and a 30-minute working time.

PART 3 - EXECUTION

3.1 COMMON REQUIREMENTS FOR ELECTRONIC SAFETY AND SECURITY INSTALLATION

- A. Comply with NECA 1.
- B. Measure indicated mounting heights to bottom of unit for suspended items and to center of unit for wall-mounting items.
- C. Headroom Maintenance: If mounting heights or other location criteria are not indicated, arrange and install components and equipment to provide maximum possible headroom consistent with these requirements.
- D. Equipment: Install to facilitate service, maintenance, and repair or replacement of components of both electronic safety and security equipment and other nearby installations. Connect in such a way as to facilitate future disconnecting with minimum interference with other items in the vicinity.
- E. Right of Way: Give to piping systems installed at a required slope.

3.2 SLEEVE INSTALLATION FOR ELECTRONIC SAFETY AND SECURITY PENETRATIONS

- A. Electronic safety and security penetrations occur when raceways, pathways, cables, wireways, or cable trays penetrate concrete slabs, concrete or masonry walls, or fire-rated floor and wall assemblies.
- B. Concrete Slabs and Walls: Install sleeves for penetrations unless core-drilled holes or formed openings are used. Install sleeves during erection of slabs and walls.
- C. Use pipe sleeves unless penetration arrangement requires rectangular sleeved opening.
- D. Fire-Rated Assemblies: Install sleeves for penetrations of fire-rated floor and wall assemblies unless openings compatible with firestop system used are fabricated during construction of floor or wall.

- E. Cut sleeves to length for mounting flush with both surfaces of walls.
- F. Extend sleeves installed in floors 2 inches above finished floor level.
- G. Size pipe sleeves to provide 1/4-inch annular clear space between sleeve and raceway or cable, unless indicated otherwise.
- H. Seal space outside of sleeves with grout for penetrations of concrete and masonry
 - 1. Promptly pack grout solidly between sleeve and wall so no voids remain. Tool exposed surfaces smooth; protect grout while curing.
- I. Interior Penetrations of Non-Fire-Rated Walls and Floors: Seal annular space between sleeve and raceway or cable, using joint sealant appropriate for size, depth, and location of joint. Comply with requirements in Division 7 Section "Joint Sealants."
- J. Fire-Rated-Assembly Penetrations: Maintain indicated fire rating of walls, partitions, ceilings, and floors at raceway and cable penetrations. Install sleeves and seal raceway and cable penetration sleeves with firestop materials. Comply with requirements in Division 7 Section "Firestopping."
- K. Roof-Penetration Sleeves: Seal penetration of individual raceways and cables with flexible boot-type flashing units applied in coordination with roofing work.
- L. Aboveground, Exterior-Wall Penetrations: Seal penetrations using [steel] [cast-iron] pipe sleeves and mechanical sleeve seals. Select sleeve size to allow for 1-inch annular clear space between pipe and sleeve for installing mechanical sleeve seals.
- M. Underground, Exterior-Wall Penetrations: Install cast-iron pipe sleeves. Size sleeves to allow for 1-inch annular clear space between raceway or cable and sleeve for installing mechanical sleeve seals.

3.3 SLEEVE-SEAL INSTALLATION

- A. Install to seal exterior wall penetrations.
- B. Use type and number of sealing elements recommended by manufacturer for raceway or cable material and size. Position raceway or cable in center of sleeve. Assemble mechanical sleeve seals and install in annular space between raceway or cable and sleeve. Tighten bolts against pressure plates that cause sealing elements to expand and make watertight seal.

3.4 FIRESTOPPING

- A. Apply firestopping to penetrations of fire-rated floor and wall assemblies for electronic safety and security installations to restore original fire-resistance rating of assembly. Firestopping materials and installation requirements are specified in Division 7 Section "Firestopping."

END OF SECTION 28 05 00

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

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. UTP cabling.
 - 2. 50/125 micrometer, multimode optical fiber cabling.
 - 3. Coaxial cabling.
 - 4. RS-232 cabling.
 - 5. RS-485 cabling.
 - 6. Low-voltage control cabling.
 - 7. Control-circuit conductors.
 - 8. Fire alarm wire and cable.
 - 9. Identification products.

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. EMI: Electromagnetic interference.
- D. IDC: Insulation displacement connector.
- E. Low Voltage: As defined in NFPA 70 for circuits and equipment operating at less than 50 V or for remote-control and signaling power-limited circuits.
- F. Open Cabling: Passing telecommunications cabling through open space (e.g., between the studs of a wall cavity).
- G. RCDD: Registered Communications Distribution Designer.
- H. UTP: Unshielded twisted pair.

1.4 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: Cable tray layout, showing cable tray route to scale, with relationship between the tray and adjacent structural, electrical, and mechanical elements. Include the following:
 1. Vertical and horizontal offsets and transitions.
 2. Clearances for access above and to side of cable trays.
 3. Vertical elevation of cable trays above the floor or bottom of ceiling structure.
 4. Load calculations to show dead and live loads as not exceeding manufacturer's rating for tray and its support elements.
- C. Qualification Data: For qualified layout technician, installation supervisor, and field inspector.
- D. Source quality-control reports.
- E. Field quality-control reports.
- F. Maintenance Data: For wire and cable to include in maintenance manuals.

1.5 QUALITY ASSURANCE

- A. 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: 50 or less.
- 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.

1.6 DELIVERY, STORAGE, AND HANDLING

- A. Test cables upon receipt at Project site.
 1. Test optical fiber cable to determine the continuity of the strand end to end. Use optical loss test set.
 2. Test each pair of UTP cable for open and short circuits.

1.7 PROJECT CONDITIONS

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

PART 2 - PRODUCTS

2.1 PATHWAYS

- A. Support of Open Cabling: 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.
- B. Cable Trays:
 - 1. Manufacturers: Subject to compliance with requirements, available manufacturers offering products that may be incorporated into the Work include, but are not limited to, the following:
 - a. Cable Management Solutions, Inc.
 - b. Cablofil Inc.
 - c. Cooper B-Line, Inc.
 - d. Cope - Tyco/Allied Tube & Conduit.
 - e. GS Metals Corp.
 - 2. Cable Tray Materials: Metal, suitable for indoors, and protected against corrosion by electroplated zinc galvanizing, complying with ASTM B 633, Type 1, not less than 0.000472 inch thick.
 - a. Basket Cable Trays: 6 inches wide and 2 inches deep. Wire mesh spacing shall not exceed 2 by 4 inches.
- C. Conduit and Boxes: Comply with requirements in Division 26 Section "Raceway and Boxes for Electrical Systems."

2.2 BACKBOARDS

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

2.3 UTP CABLE

- A. Manufacturers: Subject to compliance with requirements, provide products by one of the following:
 - 1. Belden CDT Inc.; Electronics Division.
 - 2. Berk-Tek; a Nexans company.
 - 3. CommScope, Inc.
 - 4. Draka USA.
 - 5. Genesis Cable Products; Honeywell International, Inc.
 - 6. KRONE Incorporated.
 - 7. Mohawk; a division of Belden CDT.
 - 8. Nordex/CDT; a subsidiary of Cable Design Technologies.
 - 9. Superior Essex Inc.

10. SYSTIMAX Solutions; a CommScope, Inc. brand.
11. 3M.
12. Tyco Electronics/AMP Netconnect; Tyco International Ltd.

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

1. Comply with ICEA S-90-661 for mechanical properties.
2. Comply with TIA/EIA-568-B.1 for performance specifications.
3. Comply with TIA/EIA-568-B.2, Category 6.
4. Listed and labeled by an NRTL acceptable to authorities having jurisdiction as complying with UL 444 and NFPA 70 for the following types:
 - a. Communications, General Purpose: Type CM or CMG.
 - b. Communications, Plenum Rated: Type CMP, complying with NFPA 262.
 - c. Communications, Riser Rated: Type CMR, complying with UL 1666.
 - d. Communications, Limited Purpose: Type CMX.
 - e. Multipurpose: Type MP or MPG.
 - f. Multipurpose, Plenum Rated: Type MPP, complying with NFPA 262.
 - g. Multipurpose, Riser Rated: Type MPR, complying with UL 1666.

2.4 UTP CABLE HARDWARE

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

1. American Technology Systems Industries, Inc.
2. Dynacom Corporation.
3. Hubbell Premise Wiring.
4. KRONE Incorporated.
5. Leviton Voice & Data Division.
6. Molex Premise Networks; a division of Molex, Inc.
7. Nordex/CDT; a subsidiary of Cable Design Technologies.
8. Panduit Corp.
9. Simon Co. (The).
10. Tyco Electronics/AMP Netconnect; Tyco International Ltd.

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

C. Connecting Blocks: 110-style for Category 6. Provide blocks for the number of cables terminated on the block, plus 25 percent spare. Integral with connector bodies, including plugs and jacks where indicated.

2.5 OPTICAL FIBER CABLE

A. Following:

1. Berk-Tek; a Nexans company.
2. CommScope, Inc.
3. Corning Cable Systems.
4. General Cable Technologies Corporation.
5. Mohawk; a division of Belden CDT.

6. Nordex/CDT; a subsidiary of Cable Design Technologies.
 7. Optical Connectivity Solutions Division; Emerson Network Power.
 8. Superior Essex Inc.
 9. SYSTIMAX Solutions; a CommScope, Inc. brand.
 10. 3M.
 11. Tyco Electronics/AMP Netconnect; Tyco International Ltd.
- B. Description: Multimode, 50/125-micrometer, 24 -fiber, nonconductive, tight buffer, optical fiber cable.
1. Comply with ICEA S-83-596 for mechanical properties.
 2. Comply with TIA/EIA-492AAAA-B for detailed specifications.
 3. Listed and labeled by an NRTL acceptable to authorities having jurisdiction as complying with UL 444, UL 1651, and NFPA 70 for the following types:
 - a. General Purpose, Nonconductive: Type OFN or OFNG.
 - b. Plenum Rated, Nonconductive: Type OFNP, complying with NFPA 262.
 - c. Riser Rated, Nonconductive: Type OFNR, complying with UL 1666.
 - d. General Purpose, Conductive: Type OFC or OFCG.
 - e. Plenum Rated, Conductive: Type OFCP, complying with NFPA 262.
 - f. Riser Rated, Conductive: Type OFCR, complying with UL 1666.
 4. Conductive cable shall be steel armored type.
 5. Maximum Attenuation: 3.50 dB/km at 850 nm; 1.5 dB/km at 1300 nm.
 6. Minimum Modal Bandwidth: 160 MHz-km at 850 nm; 500 MHz-km at 1300 nm.
- C. Jacket:
1. Jacket Color: Aqua for 50/125-micrometer cable.
 2. Cable cordage jacket, fiber, unit, and group color shall be according to TIA/EIA-598-B.
 3. Imprinted with fiber count, fiber type, and aggregate length at regular intervals not to exceed 40 inches.

2.6 OPTICAL FIBER CABLE HARDWARE

- A. Manufacturers: Subject to compliance with requirements, provide products by one of the following:
1. ADC.
 2. American Technology Systems Industries, Inc.
 3. Berk-Tek; a Nexans company.
 4. Corning Cable Systems.
 5. Dynacom Corporation.
 6. Hubbell Premise Wiring.
 7. Molex Premise Networks; a division of Molex, Inc.
 8. Nordex/CDT; a subsidiary of Cable Design Technologies.
 9. Optical Connectivity Solutions Division; Emerson Network Power.
 10. Siemon Co. (The).
- B. Cable Connecting Hardware: Meet the Optical Fiber Connector Intermateability Standards (FOCIS) specifications of TIA/EIA-604-2, TIA/EIA-604-3-A, and TIA/EIA-604-12. Comply with TIA/EIA-568-B.3.

1. Quick-connect, simplex and duplex, Type LC connectors. Insertion loss not more than 0.75 dB.
2. Type SFF connectors may be used in termination racks, panels, and equipment packages.

2.7 COAXIAL CABLE

- A. Manufacturers: Subject to compliance with requirements, provide products by one of the following:
1. Alpha Wire Company.
 2. Belden CDT Inc.; Electronics Division.
 3. Coleman Cable, Inc.
 4. CommScope, Inc.
 5. Draka USA.
- B. General Coaxial Cable Requirements: Broadband type, recommended by cable manufacturer specifically for broadband data transmission applications. Coaxial cable and accessories shall have 75-ohm nominal impedance with a return loss of 20 dB maximum from 7 to 806 MHz.
- C. RG-11/U: NFPA 70, Type CATV.
1. No. 14 AWG, solid, copper-covered steel conductor.
 2. Gas-injected, foam-PE insulation.
 3. Double shielded with 100 percent aluminum polyester tape and 60 percent aluminum braid.
 4. Jacketed with sunlight-resistant, black PVC or PE.
 5. Suitable for outdoor installations in ambient temperatures ranging from minus 40 to plus 85 deg C.
- D. RG59/U: NFPA 70, Type CATVR.
1. No. 20 AWG, solid, silver-plated, copper-covered steel conductor.
 2. Gas-injected, foam-PE insulation.
 3. Triple shielded with 100 percent aluminum polyester tape and 95 percent aluminum braid; covered by aluminum foil with grounding strip.
 4. Color-coded PVC jacket.
- E. RG-6/U: NFPA 70, Type CATV or CM.
1. No. 16 AWG, solid, copper-covered steel conductor; gas-injected, foam-PE insulation.
 2. Double shielded with 100 percent aluminum-foil shield and 60 percent aluminum braid.
 3. Jacketed with black PVC or PE.
 4. Suitable for indoor installations.
- F. RG59/U: NFPA 70, Type CATV.
1. No. 20 AWG, solid, copper-covered steel conductor; gas-injected, foam-PE insulation.
 2. Double shielded with 100 percent aluminum polyester tape and 40 percent aluminum braid.
 3. PVC jacket.
- G. RG59/U (Plenum Rated): NFPA 70, Type CMP.

1. No. 20 AWG, solid, copper-covered steel conductor; foam fluorinated ethylene propylene insulation.
2. Double shielded with 100 percent aluminum-foil shield and 65 percent aluminum braid.
3. Copolymer jacket.

H. NFPA and UL compliance, listed and labeled by an NRTL acceptable to authorities having jurisdiction as complying with UL 1655, and with NFPA 70 "Radio and Television Equipment" and "Community Antenna Television and Radio Distribution" Articles. Types are as follows:

1. CATV Cable: Type CATV.
2. CATV Plenum Rated: Type CATVP, complying with NFPA 262.
3. CATV Riser Rated: Type CATVR, complying with UL 1666.
4. CATV Limited Rating: Type CATVX.

2.8 COAXIAL CABLE HARDWARE

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

1. Aim Electronics; a brand of Emerson Electric Co.
2. Leviton Voice & Data Division.
3. Siemon Co. (The).

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

2.9 RS-232 CABLE

A. Standard Cable: NFPA 70, Type CM.

1. Paired, 2 pairs, No. 22 AWG, stranded (7x30) tinned copper conductors.
2. Polypropylene insulation.
3. Individual aluminum foil-polyester tape shielded pairs with 100 percent shield coverage.
4. PVC jacket.
5. Pairs are cabled on common axis with No. 24 AWG, stranded (7x32) tinned copper drain wire.
6. Flame Resistance: Comply with UL 1581.

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

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

2.10 RS-485 CABLE

A. Standard Cable: NFPA 70, Type CM.

1. Paired, 2 pairs, twisted, No. 22 AWG, stranded (7x30) tinned copper conductors.

2. PVC insulation.
3. Unshielded.
4. PVC jacket.
5. Flame Resistance: Comply with UL 1581.

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

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

2.11 LOW-VOLTAGE CONTROL CABLE

A. Paired Lock Cable: NFPA 70, Type CMG.

1. 1 pair, twisted, No. 16 AWG, stranded (19x29) tinned copper conductors.
2. PVC insulation.
3. Unshielded.
4. PVC jacket.
5. Flame Resistance: Comply with UL 1581.

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

1. 1 pair, twisted, No. 16 AWG, stranded (19x29) tinned copper conductors.
2. PVC insulation.
3. Unshielded.
4. PVC jacket.
5. Flame Resistance: Comply with NFPA 262.

C. Paired Lock Cable: NFPA 70, Type CMG.

1. 1 pair, twisted, No. 18 AWG, stranded (19x30) tinned copper conductors.
2. PVC insulation.
3. Unshielded.
4. PVC jacket.
5. Flame Resistance: Comply with UL 1581.

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

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

2.12 CONTROL-CIRCUIT CONDUCTORS

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

- B. Class 2 Control Circuits: Stranded copper, Type THHN-THWN, in raceway complying with UL 83.
- C. Class 3 Remote-Control and Signal Circuits: Stranded copper, Type TW or TF, complying with UL 83.

2.13 FIRE ALARM WIRE AND CABLE

- A. Manufacturers: Subject to compliance with requirements, available manufacturers offering products that may be incorporated into the Work include, but are not limited to, the following:
 - 1. Comtran Corp.
 - 2. Draka USA.
 - 3. Genesis Cable Products; Honeywell International, Inc.
 - 4. Rockbestos-Suprenant Cable Corporation.
 - 5. West Penn Wire/CDT; a division of Cable Design Technologies.
- B. General Wire and Cable Requirements: NRTL listed and labeled as complying with NFPA 70, Article 760.
- C. Signaling Line Circuits: Twisted, shielded pair, not less than No. 18 AWG and size as recommended by system manufacturer.
- D. Non-Power-Limited Circuits: Solid-copper conductors with 600-V rated, 75 deg C, color-coded insulation.
 - 1. Low-Voltage Circuits: No. 16 AWG, minimum.
 - 2. Multi-conductor Armored Cable: NFPA 70, Type MC, copper conductors, Type TFN/THHN conductor insulation, copper drain wire, copper armor with outer jacket with red identifier stripe, NTRL listed for fire alarm and cable tray installation, plenum rated, and complying with requirements in UL 2196 for a 2-hour rating.

2.14 IDENTIFICATION PRODUCTS

- A. Manufacturers: Subject to compliance with requirements, available manufacturers offering products that may be incorporated into the Work include, but are not limited to, the following:
 - 1. Brady Corporation
 - 2. HellermannTyton.
 - 3. Kroy LLC.
 - 4. Panduit Corp.
- B. Comply with UL 969 for a system of labeling materials, including label stocks, laminating adhesives, and inks used by label printers.
- C. Comply with requirements in Division 26 Section "Identification for Electrical Systems."

2.15 SOURCE QUALITY CONTROL

- A. Factory test UTP and optical fiber cables on reels according to TIA/EIA-568-B.1.
- B. Factory test UTP cables according to TIA/EIA-568-B.2.

- C. Factory test multimode optical fiber cables according to TIA/EIA-526-14-A and TIA/EIA-568-B.3.
- D. 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.
- E. Cable will be considered defective if it does not pass tests and inspections.
- F. Prepare test and inspection reports.

PART 3 - EXECUTION

3.1 INSTALLATION OF PATHWAYS

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

3.2 INSTALLATION OF CONDUCTORS AND CABLES

- A. Comply with NECA 1.
- B. General Requirements for Cabling:
 - 1. Comply with TIA/EIA-568-B.1.
 - 2. Comply with BICSI ITSIM, Ch. 6, "Cable Termination Practices."
 - 3. Install 110-style IDC termination hardware unless otherwise indicated.
 - 4. Terminate all conductors; no cable shall contain unterminated elements. Make terminations only at indicated outlets, terminals, and cross-connect and patch panels.
 - 5. Cables may not be spliced. Secure and support cables at intervals not exceeding 30 inches (760 mm) and not more than 6 inches (150 mm) from cabinets, boxes, fittings, outlets, racks, frames, and terminals.

6. Bundle, lace, and train conductors to terminal points without exceeding manufacturer's limitations on bending radii, but not less than radii specified in BICSI ITSIM, "Cabling Termination Practices" Chapter. Install lacing bars and distribution spools.
 7. Do not install bruised, kinked, scored, deformed, or abraded cable. Do not splice cable between termination, tap, or junction points. Remove and discard cable if damaged during installation and replace it with new cable.
 8. Cold-Weather Installation: Bring cable to room temperature before de-reeling. Heat lamps shall not be used for heating.
 9. 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 from the point of termination to maintain cable geometry.
- D. Optical Fiber Cable Installation:
1. Comply with TIA/EIA-568-B.3.
 2. Cable shall be terminated on connecting hardware that is rack or cabinet mounted.
- E. Open-Cable Installation:
1. Install cabling with horizontal and vertical cable guides in telecommunications spaces with terminating hardware and interconnection equipment.
 2. Suspend copper cable not in a wireway or pathway a minimum of 8 inches above ceilings by cable supports not more than 60 inches apart.
 3. Cable shall not be run through structural members or in contact with pipes, ducts, or other potentially damaging items.
- F. 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 72 inches long shall be neatly coiled not less than 12 inches in diameter below each feed point.
- G. 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.
- H. Separation from EMI Sources:
1. Comply with BICSI TDMM and TIA/EIA-569-A recommendations for separating unshielded copper voice and data communication cable from potential EMI sources, including electrical power lines and equipment.
 2. Separation between open communications cables or cables in nonmetallic raceways and unshielded power conductors and electrical equipment shall be as follows:
 - a. Electrical Equipment Rating Less Than 2 kVA: A minimum of 5 inches.
 - b. Electrical Equipment Rating between 2 and 5 kVA: A minimum of 12 inches.
 - c. Electrical Equipment Rating More Than 5 kVA: A minimum of 24 inches.

3. Separation between communications cables in grounded metallic raceways and unshielded power lines or electrical equipment shall be as follows:
 - a. Electrical Equipment Rating Less Than 2 kVA: A minimum of 2-1/2 inches.
 - b. Electrical Equipment Rating between 2 and 5 kVA: A minimum of 6 inches.
 - c. Electrical Equipment Rating More Than 5 kVA: A minimum of 12 inches.
4. Separation between communications cables in grounded metallic raceways and power lines and electrical equipment located in grounded metallic conduits or enclosures shall be as follows:
 - a. Electrical Equipment Rating Less Than 2 kVA: No requirement.
 - b. Electrical Equipment Rating between 2 and 5 kVA: A minimum of 3 inches.
 - c. Electrical Equipment Rating More Than 5 kVA: A minimum of 6 inches.
5. Separation between Cables and Electrical Motors and Transformers, 5 kVA or HP and Larger: A minimum of 48 inches.

3.3 FIRE ALARM WIRING INSTALLATION

- A. Comply with NECA 1 and NFPA 72.
- B. Wiring Method: Install wiring in metal raceway according to Division 26 Section "Raceway and Boxes for Electrical Systems."
 1. Install plenum cable in environmental air spaces, including plenum ceilings.
 2. Fire alarm circuits and equipment control wiring associated with the fire alarm system shall be installed in a dedicated raceway system. This system shall not be used for any other wire or cable.
- C. Wiring Method:
 1. Cables and raceways used for fire alarm circuits, and equipment control wiring associated with the fire alarm system, may not contain any other wire or cable.
 2. Fire-Rated Cables: Use of 2-hour, fire-rated fire alarm cables, NFPA 70, Types MI and CI, is not permitted.
 3. Signaling Line Circuits: Power-limited fire alarm cables shall not be installed in the same cable or raceway as signaling line circuits.
- D. Wiring within Enclosures: Separate power-limited and non-power-limited conductors as recommended by manufacturer. Install conductors parallel with or at right angles to sides and back of the enclosure. Bundle, lace, and train conductors to terminal points with no excess. Connect conductors that are terminated, spliced, or interrupted in any enclosure associated with the fire alarm system to terminal blocks. Mark each terminal according to the system's wiring diagrams. Make all connections with approved crimp-on terminal spade lugs, pressure-type terminal blocks, or plug connectors.
- E. Cable Taps: Use numbered terminal strips in junction, pull, and outlet boxes, cabinets, or equipment enclosures where circuit connections are made.
- F. Color-Coding: Color-code fire alarm conductors differently from the normal building power wiring. Use one color-code for alarm circuit wiring and another for supervisory circuits. Color-code audible alarm-indicating circuits differently from alarm-initiating circuits. Use different

colors for visible alarm-indicating devices. Paint fire alarm system junction boxes and covers red.

- G. Risers: Install at least two vertical cable risers to serve the fire alarm system. Separate risers in close proximity to each other with a minimum one-hour-rated wall, so the loss of one riser does not prevent the receipt or transmission of signals from other floors or zones.
- H. Wiring to Remote Alarm Transmitting Device: 1-inch conduit between the fire alarm control panel and the transmitter. Install number of conductors and electrical supervision for connecting wiring as needed to suit monitoring function.

3.4 CONTROL-CIRCUIT CONDUCTORS

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

3.5 CONNECTIONS

- A. Comply with requirements in Division 28 Section "Fire Detection and Alarm" for connecting, terminating, and identifying wires and cables.

3.6 FIRESTOPPING

- A. Comply with requirements in Division 07 Section "Firestopping."
- B. Comply with TIA/EIA-569-A, "Firestopping" Annex A.
- C. Comply with BICSI TDMM, "Firestopping Systems" Article.

3.7 GROUNDING

- A. For communications wiring, comply with ANSI-J-STD-607-A and with BICSI TDMM, "Grounding, Bonding, and Electrical Protection" Chapter.
- B. For low-voltage wiring and cabling, comply with requirements in Division 26 Section "Grounding and Bonding for Electrical Systems."

3.8 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."

3.9 FIELD QUALITY CONTROL

- A. Perform tests and inspections.

B. Tests and Inspections:

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

- C. Document data for each measurement. Print data for submittals in a summary report that is formatted using Table 10.1 in BICSI TDMM as a guide, or transfer the data from the instrument to the computer, save as text files, print, and submit.
- D. End-to-end cabling will be considered defective if it does not pass tests and inspections.
- E. Prepare test and inspection reports.

END OF SECTION 28 05 13

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. The work in this section shall be provided under separate contract and is included for general guidance purposes only.
- B. This Section includes a security access system consisting of a Central Station, one or more networked workstation computers, operating system and application software, and field-installed Controllers connected by a high-speed electronic data transmission network. The security access system shall have the following:

1. Access Control:

- a. Regulating access through doors.
- b. Anti-passback.
- c. Visitor assignment.
- d. Time and attendance.
- e. Surge and tamper protection.
- f. Secondary alarm annunciator.
- g. Credential cards and readers.
- h. Biometric identity verification equipment.
- i. Enrollment center.
- j. Push-button switches.
- k. RS-232 ASCII interface.
- l. Credential creation and credential holder database and management.
- m. Monitoring of field-installed devices.
- n. Reporting.

2. Security:

- a. Real-time guard tour.
- b. Time and attendance.
- c. Key tracking.
- d. Video and camera control.
- e. Interface with paging, elevator control and video surveillance (CCTV) systems.

- C. Related Sections include the following:

- 1. Division 28 Section "Video Surveillance" for interface devices and communications protocol to integrate motion detection and video camera selection and positioning into security access system.

1.3 DEFINITIONS

- A. ABA Track: Magnetic stripe that is encoded on track 2, at 75-bpi density in binary-coded decimal format; for example, 5-bit, 16-character set.
- B. CCTV: Video surveillance system.
- C. Central Station: A PC with software designated as the main controlling PC of the security access system. Where this term is presented with initial capital letters, this definition applies.
- D. Controller: An intelligent peripheral control unit that uses a computer for controlling its operation. Where this term is presented with an initial capital letter, this definition applies.
- E. CPU: Central processing unit.
- F. Credential: Data assigned to an entity and used to identify that entity.
- G. dpi: Dots per inch.
- H. DTS: Digital Termination Service: A microwave-based, line-of-sight communications provided directly to the end user.
- I. File Server: A PC in a network that stores the programs and data files shared by users.
- J. GFI: Ground fault interrupter.
- K. 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.
- L. I/O: Input/Output.
- M. LAN: Local area network.
- N. LED: Light-emitting diode.
- O. Location: A Location on the network having a PC-to-Controller communications link, with additional Controllers at the Location connected to the PC-to-Controller link with RS-485 communications loop. Where this term is presented with an initial capital letter, this definition applies.
- P. PC: Personal computer. This acronym applies to the Central Station, workstations, and file servers.
- Q. PCI Bus: Peripheral component interconnect; a peripheral bus providing a high-speed data path between the CPU and peripheral devices (such as monitor, disk drive, or network).
- R. PDF: (Portable Document Format.) The file format used by the Acrobat document exchange system software from Adobe.
- S. RF: Radio frequency.
- T. ROM: Read-only memory. ROM data are maintained through losses of power.

- U. RS-232: A TIA/EIA standard for asynchronous serial data communications between terminal devices. This standard defines a 25-pin connector and certain signal characteristics for interfacing computer equipment.
- V. RS-485: A TIA/EIA standard for multipoint communications.
- W. TCP/IP: Transport control protocol/Internet protocol incorporated into Microsoft Windows.
- X. 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.
- Y. UPS: Uninterruptible power supply.
- Z. WAN: Wide area network.
- AA. WAV: The digital audio format used in Microsoft Windows.
- BB. Wiegand: Patented magnetic principle that uses specially treated wires embedded in the credential card.
- CC. Windows: Operating system by Microsoft Corporation.
- DD. Workstation: A PC with software that is configured for specific limited security system functions.
- EE. WYSIWYG: (What You See Is What You Get.) Text and graphics appear on the screen the same as they will print.

1.4 SYSTEM DESCRIPTION

- A. System shall consist of a PC-based Central Station, one or more networked PC-based workstations, and field-installed Controllers, connected by a high-speed electronic data transmission network.
 - 1. System Software: Based on 32-bit, Microsoft Windows workstation operating system and application software. Software shall have the following capabilities:
 - a. Graphical user interface to show pull-down menus and a menu tree format that complies with interface guidelines of Microsoft Windows operating system.
 - b. System license shall be for the entire system and shall include capability for future additions that are within the indicated system size limits specified in this Section.
 - c. System shall have open architecture that allows importing and exporting of data and interfacing with other systems that are compatible with Microsoft Windows operating system.
 - d. Password-protected operator login and access.
- B. Network(s) connecting PCs and Controllers shall consist of one or more of the following:
 - 1. Direct-connected, RS-232 cable from the COM port of the Central Station to the first Controller, then RS-485 to interconnect the remainder of the Controllers at that Location.

1.5 PERFORMANCE REQUIREMENTS

- A. Security access system shall use a single database for access-control and credential-creation functions.
- B. System Network Requirements:
 - 1. Interconnect system components and provide automatic communication of status changes, commands, field-initiated interrupts, and other communications required for proper system operation.
 - 2. Communication shall not require operator initiation or response, and shall return to normal after partial or total network interruption such as power loss or transient upset.
 - 3. System shall automatically annunciate communication failures to the operator and identify the communication link that has experienced a partial or total failure.
- C. Field equipment shall include Controllers, sensors, and controls. Controllers are classified as alarm-annunciation or entry-control type.
- D. System Response to Alarms: Field device network shall provide a system end-to-end response time of 1 second(s) or less for every device connected to the system. All graphics shall be displayed, including graphics-generated map displays, on the console monitor within 5 seconds of alarm receipt at the security console. This response time shall be maintained during system heavy load.
- E. False Alarm Reduction: The design of Controllers shall contain features to reduce false alarms. Equipment and software shall comply with SIA CP-01.
- F. Error Detection: A cyclic code error detection method shall be used which shall detect single- and double-bit errors, burst errors of eight bits or less, and at least 99 percent of all other multibit and burst error conditions. Interactive or product error detection codes alone will not be acceptable. A message shall be in error if one bit is received incorrectly. System shall retransmit messages with detected errors. A two-digit decimal number shall be operator assignable to each communication link representing the number of retransmission attempts. System shall monitor the frequency of data transmission failure for display and logging.
- G. Data Line Supervision: System shall initiate an alarm in response to opening, closing, shorting, or grounding of data transmission lines.
- H. Door Hardware Interface: Coordinate with Division 08 Sections that specify door hardware required to be monitored or controlled by the security access system. The Controllers in this Section shall have electrical characteristics that match the signal and power requirements of door hardware. Integrate door hardware specified in Division 08 Sections to function with the controls and PC-based software and hardware in this Section.

1.6 SUBMITTALS

- A. Product Data: For each type of product indicated. Include operating characteristics, 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:
 - 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. 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 Part 3 "Identification" Article.
 5. Battery and charger calculations for Central Station, workstations, and Controllers.
- C. Project planning documents as specified in Part 3.
- D. Samples: For workstation outlets, jacks, jack assemblies, and faceplates for color selection and evaluation of technical features.
- E. Field quality-control test 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 of the hard-copy submittal.
 4. System installation and setup guides, with data forms to plan and record options and setup decisions.

1.7 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 a single manufacturer.
- C. Electrical Components, Devices, and Accessories: Listed and labeled as defined in NFPA 70, Article 100, by a testing agency acceptable to authorities having jurisdiction, and marked for intended use.
- D. Comply with NFPA 70, "National Electrical Code."
- E. Comply with SIA DC-01 and SIA DC-03 and SIA DC-07.

1.8 DELIVERY, STORAGE, AND HANDLING

- A. 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, 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 designations that have been assigned to materials and equipment for recording in the system labeling schedules that are generated by cable and asset management system specified in Part 2.
4. Save original manufacturer's containers and packing materials and deliver as directed under provisions covering extra materials.

1.9 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 and a relative humidity of 20 to 80 percent, non-condensing.
2. Interior, Controlled Environment: System components, except central-station control unit, installed in temperature-controlled interior environments shall be rated for continuous operation in ambient conditions of 36 to 122 deg F dry bulb and 20 to 90 percent relative humidity, non-condensing. NEMA 250, Type 1 enclosure.
3. Interior, Uncontrolled Environment: System components installed in non-temperature-controlled interior environments shall be rated for continuous operation in ambient conditions of 0 to 122 deg F dry bulb and 20 to 90 percent relative humidity, non-condensing. NEMA 250, Type 3R enclosures.
4. Exterior Environment: 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 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 85 mph and snow cover up to 24 inches (610 mm) thick. NEMA 250, Type 4X enclosures.
5. Hazardous Environment: System components located in areas where fire or explosion hazards may exist because of flammable gases or vapors, flammable liquids, combustible dust, or ignitable fibers shall be rated, listed, and installed according to NFPA 70.
6. Corrosive Environment: For system components subjected to corrosive fumes or vapors, provide NEMA 250, Type 4X enclosures.

1.10 EXTRA MATERIALS

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

1. Laser Printers: Three toner cassettes and one replacement drum unit.
2. Credential card blanks, ready for printing. Include enough credential cards for all personnel to be enrolled at the site plus additional 25 percent for future use.

PART 2 - PRODUCTS

2.1 MANUFACTURERS

- A. In other Part 2 articles where titles below introduce lists, the following requirements apply to product selection:
 - 1. Manufacturers: Subject to compliance with requirements, provide products by one of the manufacturers specified.

2.2 SECURITY ACCESS SYSTEM

- A. Manufacturers:
 - 1. Andover Controls Corporation; a Balfour Beatty Company.
 - 2. CASI-RUSCO; Subsidiary of SLC Technologies; Division of Berwind Group.
 - 3. Checkpoint Systems, Inc.
 - 4. Hirsch Electronics.
 - 5. Keyscan Inc.
 - 6. Matrix Systems, Inc.
 - 7. NexWatch; Member of Ademco Group; a Honeywell Company.
 - 8. Northern; Member of Ademco Group; a Honeywell Company.
 - 9. Radionics; Division of Detection Systems.

2.3 APPLICATION SOFTWARE

- A. System Software: Based on 32-bit, Microsoft Windows operating system and application software. Software shall have the following features:
 - 1. Multiuser multitasking to allow independent activities and monitoring to occur simultaneously at different workstations.
 - 2. Graphical user interface to show pull-down menus and a menu tree format.
 - 3. Capability for future additions within the indicated system size limits.
 - 4. Open architecture that allows importing and exporting of data and interfacing with other systems that are compatible with operating system.
 - 5. Password-protected operator login and access.
- B. Peer Computer Control Software: Shall detect a failure of a central computer, and shall cause the other central computer to assume control of all system functions without interruption of operation. Drivers shall be provided in both central computers to support this mode of operation.
- 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. Software shall have the following functions:
 - 1. Resides at the workstations, and Controllers as required to perform specified functions.
 - 2. Operate and manage peripheral devices.
 - 3. Manage files for disk I/O, including creating, deleting, and copying files; and automatically maintain a directory of all files, including size and location of each sequential and random-ordered record.
 - 4. Import custom icons into graphics views to represent alarms and I/O devices.

5. Globally link I/O so that any I/O can link to any other I/O within the same Location, without requiring interaction with the host PC. This operation shall be at the Controller.
6. Globally code I/O links so that any access-granted event can link to any I/O with the same Location without requiring interaction with the host PC. This operation shall be at the Controller.
7. Messages from PC to Controllers and Controllers to Controllers shall be on a polled network that utilizes check summing and acknowledgment of each message. Communication shall be automatically verified, buffered, and retransmitted if message is not acknowledged.
8. Selectable poll frequency and message time-out settings shall handle bandwidth and latency issues for TCP/IP, RF, and other PC-to-Controller communications methods by changing the polling frequency and the amount of time the system waits for a response.
9. Automatic and encrypted backups for database and history backups shall be automatically stored at the central control PC and at a selected workstation and encrypted with a nine-character alphanumeric password, which must be used to restore or read data contained in backup.
10. Operator audit trail for recording and reporting all changes made to database and system software.

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. Controllers shall operate as an autonomous intelligent processing unit. Controllers shall make decisions about access control, alarm monitoring, linking functions, and door locking schedules for its operation, independent of other system components. Controllers shall be part of a fully distributed processing control network. The portion of the database associated with a Controller and consisting of parameters, constraints, and the latest value or status of points connected to that Controller, shall be maintained in the Controller.
2. Functions: The following functions shall be fully implemented and operational within each Controller:
 - a. Monitoring inputs.
 - b. Controlling outputs.
 - c. Reporting of sensor and output status to Central Station on request.
 - d. Executing Controller resident programs.
 - e. Diagnosing.
3. Controller Operations at a Location:
 - a. Location: Up to 64 Controllers connected to RS-485 communications loop. Globally operating I/O linking and anti-passback functions between Controllers within the same Location without workstation intervention. Linking and anti-passback shall remain fully functional within the same Location even when the workstations are off line.
 - b. The Controllers at each Location shall be connected to a memory buffer with a capacity to store up to 10,000 events; there shall be no loss of transactions in system history files until the buffer overflows.

- c. Buffered events shall be handled in a first-in-first-out mode of operation.
 - 4. Individual Controller Operation:
 - a. Controllers shall transmit alarms, status changes, and other data to the Central Station when communications circuits are operable. If communications are not available, Controllers shall function in a stand-alone mode and operational data, including the status and alarm data normally transmitted to the Central Station, shall be stored for later transmission to the Central Station. Storage capacity for the latest 1024 events shall be provided at each Controller.
 - b. Card-reader ports of a Controller shall be custom configurable for at least 120 different card-reader or keypad formats. Multiple reader or keypad formats may be used simultaneously at different Controllers or within the same Controller.
 - c. Controllers shall provide a response to card-readers or keypad entries in less than 0.25 seconds, regardless of system size.
 - d. Controllers that are reset, or powered up from a nonpowered state, shall automatically request a parameter download and reboot to its proper working state. This shall happen without any operator intervention.
 - e. Initial Startup: When Controllers are brought on-line, database parameters shall be automatically downloaded to them. After initial download is completed, only database changes shall be downloaded to each Controller.
 - f. Failure Mode: On failure for any reason, Controllers shall perform an orderly shutdown and force Controller outputs to a predetermined failure mode state, consistent with the failure modes shown and the associated control device.
 - g. Startup After Power Failure: After power is restored, startup software shall initiate self-test diagnostic routines, after which Controllers shall resume normal operation.
 - h. Startup After Controller Failure: On failure, if the database and application software are no longer resident, Controllers shall not restart, but shall remain in the failure mode until repaired. If database and application programs are resident, Controllers shall immediately resume operation. If not, software shall be restored automatically from the Central Station.
 - 5. Communications Monitoring:
 - a. System shall monitor and report status of RS-485 communications loop of each Location.
 - b. Communication status window shall display which Controllers are currently communicating, a total count of missed polls since midnight, and which Controller last missed a poll.
 - c. Communication status window shall show the type of CPU, the type of I/O board, and the amount of RAM memory for each Controller.
 - 6. Operating systems shall include a real-time clock function that maintains seconds, minutes, hours, day, date, and month. The real-time clock shall be automatically synchronized with the controllers 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. Workstation communications shall use the following:
 - a. Direct connection using serial ports of the PC.
 - b. TCP/IP LAN network interface cards.
 - c. Dial-up modems for connections to Locations.

2. Serial Port Configuration: Each serial port used for communications shall be individually configurable for "direct communications," "modem communications incoming and outgoing," or "modem communications incoming only"; or as an ASCII output port.
 3. Multiport Communications Board: Use if more than two serial ports are needed.
 - a. Expandable and modular design. Use a 4-, 8-, or 16-serial port configuration that is expandable to 32 or 64 serial ports.
 - b. Connect the first board to an internal PCI bus adapter card.
 4. Direct serial, TCP/IP, and dial-up communications shall be alike in the monitoring or control of system, except for the connection that must first be made to a dial-up Location.
 5. TCP/IP network interface card shall have an option to set the poll frequency and message response time-out settings.
 6. PC-to-Controller and Controller-to-Controller communications (direct, dial-up, or TCP/IP) shall use a polled-communication protocol that checks sum and acknowledges each message. All communications shall be verified and buffered and retransmitted if not acknowledged.
- 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 communications 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. Dial-up Modem PC-to-Controller Communications:
1. Communication software on the PC shall supervise the PC-to-Controller communications link during dial-up modem connect times.
 2. Communication software shall be programmable to routinely poll each of the remote dial-up modem Locations, collecting event logs and verifying phone lines at time intervals that are operator selectable for each Location.
 3. System shall be programmable for dialing and connecting to all dial-up modem Locations and for retrieving the accrued history transactions on an automatic basis as often as once every 10 minutes and up to once every 9999 minutes.
 4. Failure to communicate to a dial-up Location three times in a row shall result in an alarm at the PC.
 5. Time offset capabilities shall be present so that Locations in a different geographical time zone than the host PC will be set to, and maintained at, the proper local time. This feature shall allow for geographical time zones that are ahead of or behind the host PC.
 6. The Controller connected to a dial-up modem shall automatically buffer all normal transactions until its buffer reaches 80 percent of capacity.
 7. Alarms shall be reported immediately.
 8. Dial-up modems shall be provided by manufacturer of the system. Modems used at the Controller shall be powered by the Controller. Power to the modem shall include battery backup if the Controller is so equipped.
- I. Controller-to-Controller Communications:
1. Controller-to-Controller Communications: RS-485, 4-wire, point-to-point, regenerative (repeater) communications network methodology.
 2. RS-485 communications signal shall be regenerated at each Controller.

J. Database Downloads:

1. All data transmissions from PCs to a Location, and between Controllers at a Location, shall include a complete database checksum to check the integrity of the transmission. If the data checksum does not match, a full data download shall be automatically retransmitted.
2. If a Controller is reset for any reason, it shall automatically request and receive a database download from the PC. The download shall restore data stored at the Controller to their normal working state and shall take place with no operator intervention.

K. Operator Interface:

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

- d. The second time and date shall be assigned the state that the point shall return to, when the time and date become current.
- 9. Copy command in database shall allow for like data to be copied and then edited for specific requirements, to reduce redundant data entry.

L. Operator Access Control:

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

M. Operator Commands:

- 1. Command Input: Plain-language words and acronyms shall allow operators to use the system without extensive training or data-processing backgrounds. System prompts shall be a word, a phrase, or an acronym.
 - 2. Command inputs shall be acknowledged and processing shall start in not less than [1] **<Insert number>** 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/off security lights.
 - i. Display Graphics: Used to display any graphic displays implemented in the system. Graphic displays shall be completed within 20 seconds from time of operator command.
 - 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 applications 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 twice a day through time-zone programming.
 - 4) Enable or disable cards or codes up to four times per 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.

N. Alarms:

1. System Setup:
 - a. Assign manual and automatic responses to incoming point status change or alarms.
 - b. Automatically respond to input with a link to other inputs, outputs, operator-response plans, unique sound with use of WAV files, and maps or images that graphically represent the point location.
 - c. 60-character message field for each alarm.
 - d. Operator-response-action messages shall allow message length of at least 65,000 characters, with database storage capacity of up to 32,000 messages. Setup shall assign messages to access point.
 - e. Secondary messages shall be assignable by the operator for printing to provide further information and shall be editable by the operator.
 - f. Allow 25 secondary messages with a field of 4 lines of 60 characters each.
 - g. Store the most recent 1000 alarms for recall by the operator using the report generator.
2. Software Tamper:
 - a. Annunciate a tamper alarm when unauthorized changes to system database files are attempted. Three consecutive unsuccessful attempts to log onto system shall generate a software tamper alarm.
 - b. Annunciate a software tamper alarm when an operator or other individual makes three consecutive unsuccessful attempts to invoke functions beyond their authorization level.

- c. Allow only acknowledgment of software tamper alarms.
 - 3. Read access to system transcript files shall be reserved for operators with the highest password authorization level available in system.
 - 4. Animated Response Graphics: Highlight alarms with flashing icons on graphic maps; display and constantly update the current status of alarm inputs and outputs in real time through animated icons.
 - 5. Multimedia Alarm Annunciation: WAV files to be associated with alarm events for audio annunciation or instructions.
 - 6. Alarm Handling: Each input may be configured so that an alarm cannot be cleared unless it has returned to normal, with options of requiring the operator to enter a comment about disposition of alarm. Allow operator to silence alarm sound when alarm is acknowledged.
 - 7. CCTV Alarm Interface: Allow commands to be sent to CCTV systems during alarms (or input change of state) through serial ports.
 - 8. Camera Control: Provides operator ability to select and control cameras from graphic maps.
- O. 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 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 same alarm point shall be acknowledged at same time the operator acknowledges the first alarm. Identical alarms shall be resolved when the first alarm is resolved.
 13. Alarm functions shall have priority over downloading, retrieving, and updating database from workstations and Controllers.
 14. When a reader-controlled output (relay) is opened, the corresponding alarm point shall be automatically bypassed.
- P. Monitor Display: Display text and graphic maps that include zone status integrated into the display. Colors are used for the various components and current data. Colors shall be uniform throughout the system.
1. Color Code:
 - a. FLASHING RED: Alerts operator that a zone has gone into an alarm or that primary power has failed.
 - b. STEADY RED: Alerts operator that a zone is in alarm and alarm has been acknowledged.
 - c. YELLOW: Advises operator that a zone is in access.
 - d. GREEN: Indicates that a zone is secure and that power is on.
 2. Graphics:
 - a. Support 32,000 graphic display maps and allow import of maps from a minimum of 16 standard formats from another drawing or graphics program.
 - b. Allow I/O to be placed on graphic maps by the drag-and-drop method.
 - c. Operators shall be able to view the inputs, outputs, and the point's name by moving the mouse cursor over the point on graphic map.
 - d. Inputs or outputs may be placed on multiple graphic maps. The operator shall be able to toggle to view graphic map associated with inputs or outputs.
 - e. Each graphic map shall have a display-order sequence number associated with it to provide a predetermined order when toggled to different views.
 - f. Camera icons shall have the ability to be placed on graphic maps that, when selected by an operator, will open a video window, display the camera associated with that icon, and provide pan-tilt-zoom control.
 - g. Input, output, or camera placed on a map shall allow the ability to arm or bypass an input, open or secure an output, or control the pan-tilt-zoom function of the selected camera.
- Q. 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.
- R. Report Generator Software: Include commands to generate reports for displaying, printing, and storing on disk and tape. Reports shall be stored by type, date, and time. Report printing shall be the lowest priority activity. Report generation mode shall be operator selectable but set up

initially as periodic, automatic, or on request. Include time and date printed and the name of operator generating the report. Report formats may be configured by operators.

1. Automatic Printing: Setup shall specify, modify, or inhibit the report to be generated; the time the initial report is to be generated; the time interval between reports; the end of period; and the default printer.
2. Printing on Requests: An operator may request a printout of any report.
3. Alarm Reports: Reporting shall be automatic as initially set up. Include alarms recorded by system over the selected time and information about the type of alarm (such as door alarm, intrusion alarm, tamper alarm, etc.) the type of sensor, the location, the time, and the action taken.
4. Access and Secure Reports: Document zones placed in access, the time placed in access, and the time placed in secure mode.
5. Custom Reports: Reports tailored to exact requirements of who, what, when, and where. As an option, custom report formats may be stored for future printing.
6. Automatic History Reports: Named, saved, and scheduled for automatic generation.
7. Cardholder Reports: Include data, or selected parts of the data, as well as the ability to be sorted by name, card number, imprinted number, or by any of the user-defined fields.
8. Cardholder by Reader Reports: Based on who has access to a specific reader or group of readers by selecting the readers from a list.
9. Cardholder by Access-Level Reports: Display everyone that has been assigned to the specified access level.
10. Who Is In (Muster) Report:
 - a. Emergency Muster Report: One click operation on toolbar launches report.
 - b. Cardholder Report. Contain a count of persons that are "In" at a selected Location and a count with detailed listing of name, date, and time of last use, sorted by the last reader used or by the group assignment.
11. Panel Labels Reports: Printout of control-panel field documentation including the actual location of equipment, programming parameters, and wiring identification. Maintain system installation data within system database so that they are available on-site at all times.
12. Activity and Alarm On-Line Printing: Activity printers for use at workstations; prints all events or alarms only.
13. History Reports: Custom reports that allows the operator to select any date, time, event type, device, output, input, operator, Location, name, or cardholder to be included or excluded from the report.
 - a. Initially store history on the hard disk of the host PC.
 - b. Permit viewing of the history on workstations or print history to any system printer.
 - c. The report shall be definable by a range of dates and times with the ability to have a daily start and stop time over a given date range.
 - d. Each report shall depict the date, time, event type, event description, device, or I/O name, cardholder group assignment, and cardholder name or code number.
 - e. Each line of a printed report shall be numbered to ensure that the integrity of the report has not been compromised.
 - f. Total number of lines of the report shall be given at the end of the report. If the report is run for a single event such as "Alarms," the total shall reflect how many alarms occurred during that period.
14. Reports shall have the following four options:
 - a. View on screen.
 - b. Print to system printer. Include automatic print spooling and "Print To" options if more than one printer is connected to system.

- c. "Save to File" with full path statement.
 - d. System shall have the ability to produce a report indicating status of system inputs and outputs or of inputs and outputs that are abnormal, out of time zone, manually overridden, not reporting, or in alarm.
 - 15. Custom Code List Subroutine: Allow the access codes of system to be sorted and printed according to the following criteria:
 - a. Active, inactive, or future activate or deactivate.
 - b. Code number, name, or imprinted card number.
 - c. Group, Location, access levels.
 - d. Start and stop code range.
 - e. Codes that have not been used since a selectable number of days.
 - f. In, out, or either status.
 - g. Codes with trace designation.
 - 16. The reports of system database shall allow options so that every data field may be printed.
 - 17. The reports of system database shall be constructed so that the actual position of the printed data shall closely match the position of the data on the data-entry windows.
- S. 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.
- T. Visitor Assignment:
- 1. Provide for and allow an operator to be restricted to only working with visitors. The visitor badging subsystem shall assign credentials and enroll visitors. Allow only access levels that have been designated as approved for visitors.
 - 2. Provide an automated log of visitor name, time and doors accessed, and whom visitor contacted.
 - 3. Allow a visitor designation to be assigned to a credential holder.
 - 4. Security access system shall be able to restrict the access levels that may be assigned to credentials that are issued to visitors.

5. Allow operator to recall visitors' credential holder file, once a visitor is enrolled in the system.
6. The operator may designate any reader as one that deactivates the credential after use at that reader. The history log shall show the return of the credential.
7. System shall have the ability to use the visitor designation in searches and reports. Reports shall be able to print all or any visitor activity.

U. Time and Attendance:

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

V. 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.

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

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

6. Personnel Search Engine: A report generator with capabilities such as search by last name, first name, group, or any predetermined user-defined data field; by codes not used in definable number of days; by skills; or by seven other methods.
7. Multiple Deactivate Dates for Cards: User-defined fields to be configured as additional stop dates to deactivate any cards assigned to the cardholder.
8. Batch card printing.
9. Default card data can be programmed to speed data entry for sites where most card data are similar.
10. Enhanced ACSII File Import Utility: Allows the importing of cardholder data and images.
11. Card Expire Function: Allows readers to be configured to deactivate cards when a card is used at selected devices.

2.4 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. All data entry shall be automatically checked for duplicate and illegal data and shall verify that data are in a valid format.
 4. Provide a memo or note field for each item that is stored in database, allowing the storing of information about any defining characteristics of the item. Memo field is used for noting the purpose the item was entered for, reasons for changes that were made, and the like.
- C. File Management:
 1. Provide database backup and restoration system, allowing selection of storage media, including 3.5-inch floppy disk, Zip and Jaz drives, and designated network resources.
 2. Provide manual and automatic mode of backup operations. The number of automatic sequential backups before the oldest backup becomes overwritten; FIFO mode shall be operator selectable.
 3. Backup program shall provide manual operation from any PC on the LAN and shall operate while system remains operational.
- D. Operator Passwords:
 1. Software shall support up to 32,000 individual system operators, each with a unique password.

2. Operator Password: Minimum eight alphanumeric characters.
 3. Allow passwords to be case sensitive.
 4. Passwords shall not be displayed when entered.
 5. Provide each password with a unique and customizable password profile, and allow several operators to share a password profile. Include the following features in the password profile:
 - a. Allow for at least 32,000 operator password profiles.
 - b. Predetermine the highest-level password profile for access to all functions and areas of program.
 - c. Allow or disallow operator access to any program operation, including the functions of View, Add, Edit, and Delete.
 - d. Restrict which doors an operator can assign access to.
 6. Operators shall use a user name and password to log on to system.
 - a. This user name and password is used to access database areas and programs as determined by the associated profile.
 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, without assigning that person a card or code, for data tracking or photo ID purposes.
 9. Cardholder Tracing: Allow for selection of cardholder for tracing. Make a special audible and visual annunciation at control station when a selected card or code is used at a designated code reader. Annunciation shall include an automatic display of the cardholder image.
 10. Allow each cardholder to be given either an unlimited number of uses or a number from 1 to 9998 that regulates the number of times the card can be used before it is automatically deactivated.
 11. Provide for cards and codes to be activated and deactivated manually or automatically by date. Provide for multiple deactivate dates to be preprogrammed.
- F. Security Access Integration:
1. Photo ID badging and photo verification shall use same database as the security access and may query data from cardholder, group, and other personal information to build a custom ID badge.

2. 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 that has possession of 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 particular doors.
- I. Operator Comments:
1. With the press of one appropriate button on toolbar, the user shall be permitted to make operator comments into history at anytime.
 2. Automatic prompting of operator comment shall occur before the resolution of each alarm.
 3. Operator comments shall be recorded by time, date, and operator number.
 4. Comments shall be sorted and viewed through reports and history.
 5. The operator may enter comments in two ways; either or both may be used:
 - a. Manually entered through keyboard data entry (typed), up to 65,000 characters per each alarm.
 - b. Predefined and stored in database for retrieval on request.
 6. System shall have a minimum of 999 predefined operator comments with up to 30 characters per comment.
- 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 1 of 32,000 group names to an access authorization.
 3. Make provision in software to deactivate and reactivate all access authorizations assigned to a particular group.
 4. Allow sorting of history reports and code list printouts by group name.
- K. Time Zones:
1. Each zone consists of a start and stop time for 7 days of the week and three holiday schedules. A time zone is assigned to inputs, outputs, or access levels to determine when an input shall automatically arm or disarm, when an output automatically opens or secures, or when access authorization assigned to an access level will be denied or granted.
 2. Up to four time zones may be assigned to inputs and outputs to allow up to four arm or disarm periods per day or four lock or unlock periods per day; up to three holiday override schedules may be assigned to a time zone.
 3. Data-entry window shall display a dynamically linked bar graph showing active and inactive times for each day and holiday, as start and stop times are entered or edited.
 4. System shall have the capacity for 2048 time zones for each Location.

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 holidays.
3. Three separate holiday schedules may be applied to a time zone.
4. Holidays have an option to be designated as occurring on the designated date each year. These holidays remain in system and will not be purged.
5. Holidays not designated to occur each year shall be automatically purged from database after the date expires.

M. Access Levels:

1. System shall allow for the creation up to 32,000 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 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 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.

2.5 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.
- 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.

2.6 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 2.4 GHz.
 1. Memory: 64 GB of usable installed memory, expandable to a minimum of 256 GB without additional chassis or power supplies.
 2. Power Supply: Minimum capacity of 250 W.
 3. Real-Time Clock:
 - a. Accuracy: Plus or minus 1 minute per month.
 - b. Time Keeping Format: 24-hour time format including seconds, minutes, hours, date, day, and month; resettable by software.
 - c. Provide automatic time correction once every 24 hours by synchronizing clock with the Central Station.
 4. Serial Ports: Provide two RS-232-F serial ports for general use, with additional ports as required. Data transmission rates shall be selectable under program control.
 5. Parallel Port: An enhanced parallel port.
 6. LAN Adapter Card: 10/1000 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 17 inches, with a minimum resolution of 1280 by 1024 pixels, noninterlaced, and a maximum dot pitch of 0.28 mm. The video card shall support at least 256 colors at a resolution of 1280 by 1024 at a minimum refresh rate of 70 Hz.
 9. Keyboard: With a minimum of 64 characters, standard ASCII character set based on ANSI X3.154.
 10. Mouse: Standard, compatible with the installed software.
 11. Disk storage shall include the following, each with appropriate controller:
 - a. Minimum 2 TB hard disk, maximum average access time of 10 ms.
 12. Printer:
 - a. Laser printer with minimum resolution of 600 dpi.
 - b. RAM: 64 GB, minimum.

- c. Printing Speed: Minimum 24 pages per minute.
 - d. Paper Handling: Automatic sheet feeder.
- 13. Interface: Bidirectional parallel, and universal serial bus.
- 14. LAN Adapter Card: 10/1000 Mbps internal network interface card.
- C. Redundant Workstation: One identical redundant workstation, connected in a hot standby, peer configuration. This workstation shall automatically maintain its own copies of system software, application software, and data files. System transactions and other activities that alter system data files shall be updated to system files of redundant workstation in near real time. If its associated workstation fails, redundant workstation shall assume control immediately and automatically.

2.7 FIXED MAP DISPLAY

- A. A fixed map display shall show layout of the protected facilities. Zones corresponding to those monitored by system shall be highlighted on the display. Status of each zone shall be displayed using LEDs as required within each designated zone. An LED test switch shall be provided on the map display.

2.8 CONTROLLERS

- A. Controllers: Intelligent peripheral control unit, complying with UL 294, that stores time, date, valid codes, access levels, and similar data downloaded from the Central Station or workstation for controlling its operation.
- B. Subject to compliance with requirements in this Article, manufacturers may use multipurpose Controllers.
- C. Battery Backup: Sealed, lead acid; sized to provide run time during a power outage of 90 minutes, complying with UL 924.
- D. Alarm Annunciation Controller:
 - 1. The Controller shall automatically restore communication within 10 seconds after an interruption with the field device network.
 - a. Inputs: Monitor dry contacts for changes of state that reflect alarm conditions. Provides at least eight alarm inputs, which are suitable for wiring as normally open or normally closed contacts for alarm conditions.
 - b. Alarm-Line Supervision:
 - 1) Supervise the alarm lines by monitoring each circuit for changes or disturbances in the signal 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 personal identity verification devices, door strikes, magnetic latches, gate and door operators, and exit push-buttons.
 - a. Operate as a stand-alone portal Controller using the downloaded database during periods of communication loss between the Controller and the field-device network.
 - b. Accept information generated by the entry-control devices; automatically process this information to determine valid identification of the individual present at the portal:
 - 1) On authentication of the credentials or information presented, check privileges of the identified individual, allowing only those actions granted as privileges.
 - 2) Privileges shall include, but not be limited to, time of day control, day of week control, group control, and visitor escort control.
 - c. Maintain a date-, time-, and Location-stamped record of each transaction. A transaction is defined as any successful or unsuccessful attempt to gain access through a controlled portal by the presentation of credentials or other identifying information.
2. Inputs:
 - a. Data from entry-control devices; use this input to change modes between access and secure.
3. Outputs:
 - a. Indicate success or failure of attempts to use entry-control devices and make comparisons of presented information with stored identification information.
 - b. Grant or deny entry by sending control signals to portal-control devices and mask intrusion alarm annunciation from sensors stimulated by authorized entries.
 - c. Maintain a date-, time-, and Location-stamped record of each transaction and transmit transaction records to the Central Station.
 - d. Door Prop Alarm: If a portal is held open for longer than 20 seconds, alarm sounds.
4. With power supplies sufficient to power at voltage and frequency required for field devices and portal-control devices.
5. Data Line Problems: For periods of loss of communications 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: Premium, valve-regulated, recombinant-sealed, lead-calcium battery; spill proof; with a full 1-year warranty and a pro rata 19-year warranty.

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. Backup Power Supply Capacity: 90 minutes of battery supply. Submit battery and charger calculations.
- c. 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 LEDs 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.

2.9 KEYPADS

- A. Designed for use with unique combinations of alphanumeric and other symbols as an Identifier. Keys of keypads shall contain an integral alphanumeric/special symbol keyboard with symbols arranged in ascending ASCII-code ordinal sequence. Communications protocol shall be compatible with Controller.
 - 1. Keypad display or enclosure shall limit viewing angles of the keypad as follows:
 - a. Maximum Horizontal Viewing Angle: 5 degrees or less off in either direction of a vertical plane perpendicular to the plane of the face of the keypad display.
 - b. Maximum Vertical Viewing Angle: 15 degrees or less off in either direction of a horizontal plane perpendicular to the plane of the face of the keypad display.
 - 2. Duress Codes: Provide duress situation indication by entering a special code.

2.10 CARD READERS

- A. Power: Card reader shall be powered from its associated Controller, including its standby power source.
- B. Response Time: Card reader shall respond to passage requests by generating a signal that is sent to the Controller. Response time shall be 800 ms or less, from the time the card reader finishes reading the credential card until a response signal is generated.
- C. Enclosure: Suitable for surface, semiflush, or pedestal mounting. Mounting types shall additionally be suitable for installation in the following locations:
 - 1. Indoors, controlled environment.
 - 2. Indoors, uncontrolled environment.
 - 3. Outdoors, with built-in heaters or other cold-weather equipment to extend the operating temperature range as needed for operation at the site.
- D. Display: LED or other type of visual indicator display shall provide visual and audible status indications and user prompts. Indicate power on/off, whether user passage requests have been accepted or rejected, and whether the door is locked or unlocked.

- E. Stripe Swipe Readers: Bidirectional, reading cards swiped in both directions, powered by the Controller.
 - 1. 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 in a humidity range of 10 to 90 percent.
- F. Bar-Code Reader: Set up for Code 128.
- G. Insert Readers: Requiring the card to be inserted from the bottom, powered by the Controller.
- H. 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 contact with to at least 6 inches from the reader.
- I. Keypad and Swipe Reader Combination: Designed to require an entry on the keypad before presenting the credential card.
 - 1. Keypad: Allow the entry of four alphanumeric characters that are associated with a specific credential. Keys of 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: 5 degrees or less off in either direction of a vertical plane perpendicular to the plane of the face of the keypad display.
 - b. Maximum Vertical Viewing Angle: 15 degrees or less off in either direction of a horizontal plane perpendicular to the plane of the face of the keypad display.
 - 2. Swipe Reader: Set up for 26-bit data cards. Comply with SIA AC-01.

2.11 ENROLLMENT CENTER

- 1. Autostar Technology Pte Ltd.
 - 2. Applied Wireless Identifications Group, Inc.
 - 3. DMP.
 - 4. IDenticard Systems, Inc.
 - 5. ISONAS.
 - 6. Ultra Electronics Limited.
- 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. 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 operating system.
- E. 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 the credential holder is assigned to. 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 same badge, including, but not be limited to, bar codes, digital photos, and signatures.
 7. Support transparent backgrounds so that image is only surrounded by the intended background, but not its immediate background.
- F. 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.
- G. 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.
- H. 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 7810, ISO 7811-1, ISO 7811-2, ISO 7811-3, and ISO 7811-6. 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. 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 proximity 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; dimensionally stable so that an undamaged card with deformations resulting from normal use is 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) With phosphorous ink as a security enhancement.
 - 2) 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 5 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.
- I. Card-Making Equipment: Consisting of a workstation, video camera, video-imaging equipment, and a printer.
- 1. Camera: NTSC color standard, RGB video output, 470 lines minimum horizontal resolution, and automatic white balance with full rated output under illumination of 0.5 fc.
 - 2. Video Imaging: Live-image capture software and hardware and a digital signature capture pad.
 - 3. Standard workstation, modified as follows:
 - a. Redundant workstation is not required.
 - b. Printer is not required.
 - c. UPS is not required.
 - d. Sound card is not required.
 - 4. Printer: Dye-sublimation resin thermal transfer, 300 dpi resolution, 16.7 million colors, accepting cards ranging in size from 2.1 by 3 inches to 2.6 by 3.7 inches and having card thickness ranging from 0.020 to 0.060 inch. Printer shall have options for encoding magnetic stripe using tracks 1, 2, and 3. Throughput shall be not less than 60 seconds per card.

2.12 PUSH-BUTTON SWITCHES

- A. Available Manufacturers:

1. Securitron Magnalock Corporation; an ASSA ABLOY Group Company.
- B. Push-Button Switches: Momentary-contact back-lighted push buttons, with stainless-steel switch enclosures.
 1. Electrical Ratings:
 - a. Minimum continuous current rating of 10 A at 120 V ac or 5 A at 240-V ac.
 - b. Contacts that will make 720 VA at 60 A and that will break at 720 VA at 10 A.
 2. Enclosures: Flush or surface mounting. Push buttons shall be suitable for flush mounting in the switch enclosures.
 3. Enclosures shall additionally be suitable for installation in the following locations:
 - a. Indoors, controlled environment.
 - b. Indoors, uncontrolled environment.
 - c. Outdoors.
 4. Power: Push-button switches shall be powered from their associated Controller, using dc control.

2.13 DOOR AND GATE 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 shall report a forced entry. Power and signal shall be from the Controller. Electric strikes are specified in Division 08 "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."
- E. Vehicle Gate Operator: Interface electrical operation of gate with controls of this Section. Vehicle gate operators shall be connected, monitored, and controlled, by the security access Controllers. Vehicle gate and accessories are specified in Division 32 Section "Chain Link Fences and Gates."

2.14 RS-232 ASCII INTERFACE SPECIFICATIONS

- A. ASCII interface shall allow RS-232 connections to be made between the control station operating as the host PC and any equipment that will accept RS-232 ASCII command strings, such as CCTV switchers, intercoms, and paging systems.
 1. Each alarm input in system shall allow for individual programming to output up to four unique ASCII character strings through two different COM ports on the host PC.

2. Each input shall have the ability to be defined to transmit a unique ASCII string for alarm and one for restore through one COM port, and a unique ASCII string for a nonalarm abnormal condition and one for a normal condition through the same or different COM port.
 3. The predefined ASCII character strings shall have the ability to be up to 420 characters long with full use of all the ASCII control characters, such as return or line feed. The character strings shall be defined in database of system and then assigned to the appropriate inputs.
 4. The COM ports of the host PC used to interface with external equipment shall be defined in the setup portion of the software. The COM port's baud rate, word length, stop bits, and parity shall be definable in the software to match that of the external equipment.
- B. Pager System Interface: Alarms shall be able to activate a pager system with customized message for each input alarm.
1. RS-232 output shall be capable of connection to a pager interface that can be used to call a paging system or service and send a signal to a portable pager. System shall allow an individual alphanumeric message per alarm input to be sent to the paging system. This interface shall support both numeric and alphanumeric pagers.
- C. Alarm System Interface:
1. RS-232 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 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 suffix.

2.15 VIDEO AND CAMERA CONTROL

- A. Control station or designated workstation displays live video from a CCTV source.
1. Control Buttons: On the display window, with separate control buttons to represent Left, Right, Up, Down, Zoom In, Zoom Out, Scan, and a minimum of two custom command auxiliary controls.
 2. Provide at least seven icons to represent different types of cameras, with ability to import custom icons. Provide option for display of icons on graphic maps to represent their physical location.
 3. Provide the alarm-handling window with a command button that will display the camera associated with the alarm point.
- B. Display mouse-selectable icons representing each camera source, to select source to be displayed. For CCTV sources that are connected to a video switcher, control station shall automatically send control commands through a COM port to display the requested camera when the camera icon is selected.
- C. Allow cameras with preset positioning to be defined by displaying a different icon for each of the presets. Provide control with Next and Previous buttons to allow operator to cycle quickly through the preset positions.

2.16 CABLES

A. Available Manufacturers:

1. Anixter, Inc.
2. Belden Inc.; Electronics Division.
3. Berk-Tek; a Nexans Company.
4. BIW Cable Systems; a Draka USA Company.
5. Champlain Cable Corporation.
6. Chromatic Technologies; a Draka USA Company.
7. Coleman Cable.
8. General Cable Technologies Corporation.
9. KRONE Incorporated.
10. Mohawk/CDT; a division of Cable Design Technologies.
11. West Penn Wire/CDT; a division of Cable Design Technologies.

B. Comply with Division 28 Section "Conductors and Cables for Electronic Safety and Security."

C. PVC-Jacketed, RS-232 Cable: Paired, 2 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. Pairs are cabled on common axis with No. 24 AWG, stranded (7x32) tinned copper drain wire.

1. NFPA 70, Type CM.
2. Flame Resistance: UL 1581 Vertical Tray.

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

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

E. RS-485 communications require 2 twisted pairs, with a distance limitation of 4000 feet.

F. PVC-Jacketed, RS-485 Cable: Paired, 2 pairs, twisted, No. 22 AWG, stranded (7x30) tinned copper conductors, PVC insulation, unshielded, PVC jacket, and NFPA 70, Type CMG.

G. Plenum-Type, RS-485 Cable: Paired, 2 pairs, No. 22 AWG, stranded (7x30) tinned copper conductors, fluorinated-ethylene-propylene insulation, unshielded, and fluorinated-ethylene-propylene jacket.

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

H. Multiconductor, PVC Readers and Wiegand Keypads Cables: 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.

1. NFPA 70, Type CMG.
2. Flame Resistance: UL 1581 Vertical Tray.
3. For TIA/EIA-RS-232 applications.

- I. Paired PVC Readers and Keypads Cable: Paired, 3 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.
 - 1. NFPA 70, Type CM.
 - 2. Flame Resistance: UL 1581 Vertical Tray.
- J. Plenum-Type, Multiconductor, Readers and Keypads Cable: 6 conductors, No. 20 AWG, stranded (7x28) tinned copper conductors, fluorinated-ethylene-propylene insulation, overall aluminum foil-polyester tape shield with 100 percent shield coverage plus tinned copper braid shield with 85 percent shield coverage, and fluorinated-ethylene-propylene jacket.
 - 1. NFPA 70, Type CMP.
 - 2. Flame Resistance: NFPA 262 Flame Test.
- K. Plenum-Type, Paired Lock Cable: 1 pair, twisted, No. 16 AWG, stranded (19x29) tinned copper conductors, PVC insulation, unshielded, and PVC jacket.
 - 1. NFPA 70, Type CMP.
 - 2. Flame Resistance: NFPA 262 Flame Test.
- L. Plenum-Type, Paired Lock Cable: 1 pair, twisted, No. 18 AWG, stranded (19x30) tinned copper conductors, fluorinated-ethylene-propylene insulation, unshielded, and plastic jacket.
 - 1. NFPA 70, Type CMP.
 - 2. Flame Resistance: NFPA 262 Flame Test.
- M. Plenum-Type, Paired Input Cable: 1 pair, twisted, No. 22 AWG, stranded (7x30) tinned copper conductors, fluorinated-ethylene-propylene insulation, aluminum foil-polyester tape shield (foil side out), with No. 22 AWG drain wire, 100 percent shield coverage, and plastic jacket.
 - 1. NFPA 70, Type CMP.
 - 2. Flame Resistance: NFPA 262 Flame Test.
- N. Plenum-Type, Paired AC Transformer Cable: 1 pair, twisted, No. 18 AWG, stranded (19x30) tinned copper conductors, fluorinated-ethylene-propylene insulation, unshielded, and plastic jacket.
 - 1. NFPA 70, Type CMP.
 - 2. Flame Resistance: NFPA 262 Flame Test.

2.17 TRANSFORMERS

- A. NFPA 70, Class II control transformers, NRTL listed. Transformers for security access-control system shall not be shared with any other system.

2.18 CABLE AND ASSET MANAGEMENT

- A. Available Manufacturers:
 - 1. IMAP Textron; Division of Greenlee Textron.
 - 2. Total Wire Software Company, Inc.

- B. Computer-based cable and asset management system, with fully integrated database and graphic capabilities, complying with requirements in TIA/EIA-606.
 - 1. Document physical characteristics by recording the network, asset, user, TIA/EAI details, device configurations, and exact connections between equipment and cabling.
 - a. Manage the physical layer of security system.
 - b. List device configurations.
 - c. List and display circuit connections.
 - d. Record firestopping data.
 - e. Record grounding and bonding connections and test data.
 - 2. Information shall be presented in database view, schematic plans, or technical drawings.
 - a. Microsoft Visio Technical Drawing shall be used as drawing and schematic plans software. Drawing symbols, system layout, and design shall comply with SIA AG-01.
 - 3. System shall interface with the following testing and recording devices:
 - a. Direct upload tests from circuit testing instrument into the PC.
 - b. Direct download circuit labeling into labeling printer.
- C. Software shall be designed for Microsoft Windows of same version as security access system's Central Station and workstations and shall be installed on the designated PC, using a hard drive dedicated only to this management function. Hard-drive capacity shall be not less than 50 GB.

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 EIA/TIA-606, "Administration Standard for the Telecommunications Infrastructure of Commercial Buildings."
- C. Obtain detailed Project planning forms from manufacturer of access-control system; develop custom forms to suit Project. Fill in all data available from Project plans and specifications and publish as Project planning documents for review and approval.

1. Record setup data for control station and workstations.
 2. For each Location, record setup of Controller features and access requirements.
 3. Propose start and stop times for time zones and holidays, and match up access levels for doors.
 4. Set up groups, 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.
- 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 Contracting."
- B. Install cables and wiring according to requirements in Division 28 Section "Conductors and Cables for Electronic Safety and Security."
- C. Wiring Method: Install wiring in raceway and cable tray except within consoles, cabinets, desks, and counters. Conceal raceway and wiring except in unfinished spaces.
- D. Install LAN cables using techniques, practices, and methods that are consistent with Category 6 rating of components and that ensure Category 6 performance of completed and linked signal paths, end to end.
- E. Install cables without damaging conductors, shield, or jacket.
- F. Boxes and enclosures containing security system components or cabling, and which are easily accessible to employees or to the public, shall be provided with a lock. Boxes above ceiling level in occupied areas of the building shall not be considered to be accessible. Junction boxes and small device enclosures below ceiling level and easily accessible to employees or the public shall be covered with a suitable cover plate and secured with tamperproof screws.
- G. Install end-of-line resistors at the field device location and not at the Controller or panel location.

3.4 CABLE APPLICATION

- A. Comply with EIA/TIA-569, "Commercial Building Standard for Telecommunications Pathways and Spaces."
- B. Cable application requirements are minimum requirements and shall be exceeded if recommended or required by manufacturer of system hardware.

- C. RS-232 Cabling: Install at a maximum distance of 50 feet.
- D. RS-485 Cabling: Install at a maximum distance of 4000 feet.
- 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 feet, and install No. 20 AWG wire if maximum distance is 500 feet.
 - 3. For greater distances, install "extender" or "repeater" modules recommended by manufacturer of the Controller.
 - 4. Install minimum No. 18 AWG shielded cable to readers and keypads that draw 50 mA or more.
- F. Install minimum No. 16 AWG cable from Controller to electrically powered locks. Do not exceed 250 feet.
- G. Install minimum No. 18 AWG ac power wire from transformer to Controller, with a maximum distance of 25 feet.

3.5 GROUNDING

- A. Comply with Division 26 Section "Grounding and Bonding for Electrical Systems."
- B. Comply with IEEE 1100, "Power and Grounding Sensitive Electronic Equipment."
- C. Ground cable shields, drain conductors, and equipment to eliminate shock hazard and to minimize ground loops, common-mode returns, noise pickup, cross talk, and other impairments.
- D. 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 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, fob, 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.
- B. Using cable and asset management software specified in Part 2, 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 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

- A. Develop, install, and test software and databases for the complete and proper operation of systems involved. Assign software license to Owner.

3.9 FIELD QUALITY CONTROL

- A. Manufacturer's Field Service: Engage a factory-authorized service representative to inspect, test, and adjust] field-assembled components and equipment installation, including connections, and to assist in field testing. Report results in writing.
- B. Testing Agency: Engage a qualified testing and inspecting agency to perform field tests and inspections and prepare test reports:
- C. Perform the following field tests and inspections and prepare test reports:
 - 1. LAN Cable Procedures: Inspect for physical damage and test each conductor signal path for continuity and shorts. Use Class 2, bidirectional, Category 5 tester. Test for faulty connectors, splices, and terminations. Test according to TIA/EIA-568-1, "Commercial Building Telecommunications Cabling Standards - Part 1 General Requirements." Link performance for UTP cables must comply with minimum criteria in TIA/EIA-568-B.
 - 2. Test each circuit and component of each system. Tests shall include, but are not limited to, measurements of power supply output under maximum load, signal loop resistance, and leakage to ground where applicable. System components with battery backup shall be operated on battery power for a period of not less than 10 percent of the calculated battery operating time. Provide special equipment and software if testing requires special or dedicated equipment.
 - 3. Operational Test: After installation of cables and connectors, demonstrate product capability and compliance with requirements. Test each signal path for end-to-end performance from each end of all pairs installed. Remove temporary connections when tests have been satisfactorily completed.

- D. Remove and replace malfunctioning devices and circuits and retest as specified above.

3.10 STARTUP SERVICE

- A. Engage a factory-authorized service representative to supervise and assist with startup service. Complete installation and startup checks according to approved procedures that were developed in "Preparation" Article and with manufacturer's written instructions.
 - 1. 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 Owner's maintenance personnel to adjust, operate, and maintain security access system. Refer to 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 28 13 00

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. The work in this section shall be provided under separate contract and is included for general guidance purposes only.
- B. This Section includes video surveillance system consisting of cameras, data transmission wiring, and a control station with its associated equipment.
- C. Video surveillance system shall be integrated with monitoring and control system specified in Division 28 Section "Access Control" that specifies systems integration.

1.3 DEFINITIONS

- A. AGC: Automatic gain control.
- B. B/W: Black and white.
- C. CCD: Charge-coupled device.
- D. MPEG: Moving picture experts group.
- E. NTSC: National Television System Committee.
- F. UPS: Uninterruptible power supply.

1.4 SUBMITTALS

- A. Product Data: For each type of product indicated, 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 for signal transmission and control. Show cable types and sizes.
 - 2. Dimensioned plan and elevations of equipment racks, control panels, and consoles. Show access and workspace requirements.
 - 3. UPS: Sizing calculations.
 - 4. Wiring Diagrams: Power, signal, and control wiring, and grounding.

- 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. Field quality-control test reports.
- E. 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.
- F. Warranty: Special warranty specified in this Section.

1.5 QUALITY ASSURANCE

- A. Electrical Components, Devices, and Accessories: Listed and labeled as defined in NFPA 70, Article 100, by a testing agency acceptable to authorities having jurisdiction, and marked for intended use.
- 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.

1.6 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 and a relative humidity of 20 to 80 percent, non-condensing.
 - 2. Interior, Controlled Environment: System components, except central-station control unit, installed in temperature-controlled interior environments shall be rated for continuous operation in ambient temperatures of 36 to 122 deg F dry bulb and 20 to 90 percent relative humidity, non-condensing. NEMA 250, Type 1 enclosures.
 - 3. Interior, Uncontrolled Environment: System components installed in non- temperature-controlled interior environments shall be rated for continuous operation in ambient temperatures of 0 to 122 deg F dry bulb and 20 to 90 percent relative humidity, non-condensing. NEMA 250, Type 3R enclosures.
 - 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 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 85 mph and snow cover up to 24 inches thick. NEMA 250, Type 4 enclosures.

1.7 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 MANUFACTURERS

- A. In other Part 2 articles where titles below introduce lists, the following requirements apply to product selection:

1. Manufacturers: Subject to compliance with requirements, provide products by one of the manufacturers specified.

2.2 SYSTEM REQUIREMENTS

- A. Video signal format shall comply with the NTSC standard composite video, interlaced. 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 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.

2.3 STANDARD CAMERAS

- A. Manufacturers:
1. ADEMCO Video; Pittway Corporation.
 2. AXCESS Inc.
 3. Crest Electronics, Inc.
 4. General Electric.
 5. Hitachi Visual Technologies.
 6. JVC Professional Products.
 7. Panasonic Security Systems Group.
 8. Pelco.
 9. Philips Communication, Security & Imaging; Philips Electronics N.V.
 10. Safety Vision.
 11. Samsung Opto-Electronics America, Inc.
 12. SANYO Fisher Company; SANYO North America Corporation.
 13. Sony.
 14. Sensormatic Electronics Corporation.
 15. Silent Witness Enterprises Ltd.

16. Toshiba Security Products.
17. Vicon Industries, Inc.

B. Automatic Color Dome Camera: Assembled and tested as a manufactured unit, containing a dome assembly, color camera, motorized pan and tilt, zoom lens, and receiver/driver.

1. Comply with UL 639. Size shall be CCD 1/4".
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 the 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 1.0 lux at F1.4 in color mode, 0.03 lux at F1.4 in black/white mode with the camera AGC off.
7. Manually selectable modes for backlight compensation or normal lighting.
8. 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.
 - a. Panning Rotation: 0 to 355 degrees, with adjustable stops.
 - b. Tilt Movement: 90 degrees, plus or minus 5 degrees, with adjustable stops.
 - c. Speed: 12 degrees per second in both horizontal and vertical planes.
 - d. Wiring: Factory prewired for camera and zoom lens functions and pan-and-tilt power and control.
 - e. Built-in encoders or potentiometers for position feedback, and thermostat-controlled heater.
 - f. Pan-and-tilt unit shall be available with preset positioning capability to recall the position of a specific scene.
9. Preset positioning: 8 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.
10. Scanning Synchronization: Determined by external synch over the coaxial cable. Camera shall revert to internally generated synchronization on loss of external synch signal.
11. White Balance: Auto-tracing white balance, with manually settable fixed balance option.
12. Motion Detector: Built-in digital.
13. Dome shall support multiplexed control communications using coaxial cable recommended by manufacturer.
14. Power supply: 24 VAC.

2.4 REINFORCED DOME CAMERAS

A. Available Manufacturers:

1. Extreme CCTV, Inc.

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.

2.5 LENSES

A. Manufacturers:

1. ADEMCO Video; Pittway Corporation.
2. AXCESS Inc.
3. Crest Electronics, Inc.
4. General Electric.
5. Hitachi Visual Technologies.
6. JVC Professional Products.
7. Panasonic Security Systems Group.
8. Pelco.
9. Philips Communication, Security & Imaging; Philips Electronics N.V.
10. Safety Vision.
11. Samsung Opto-Electronics America, Inc.
12. SANYO Fisher Company; SANYO North America Corporation.
13. Sony.
14. Sensormatic Electronics Corporation.
15. Silent Witness Enterprises Ltd.
16. Toshiba Security Products.
17. Vicon Industries, Inc.

B. Description: Optical-quality coated optics, 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 Lenses: With calibrated focus ring.
3. Zoom Lenses: Motorized, remote-controlled units, 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.

2.6 POWER SUPPLIES

- A. Power Supplies: Low-voltage power supplies matched for voltage and current requirements of cameras and accessories, type as recommended by camera, infrared illuminator and lens manufacturer.

1. Enclosure: NEMA 250, Type 1.

2.7 INFRARED ILLUMINATORS

- A. Available Manufacturers:

1. Merit Li-Lin Ent. Co., Ltd.
2. Rainbow CCTV; International Space Optics, S.A.
3. Ultrak, Inc.
4. Visiontech.
5. Watec America Corporation.

- B. Description: Lighting fixtures that emit light only in the infrared spectrum, suitable for use with cameras indicated, for nighttime surveillance, without emitting visible light.

1. Field-Selectable Beam Patterns: Narrow, medium, and wide.
2. Rated Lamp Life: More than 8000 hours
3. Power Supply: 120-V ac.

- C. Area Coverage: Illumination to 150 feet in a narrow beam pattern.

- D. Exterior housings shall be suitable for same environmental conditions as associated camera.

2.8 CAMERA-SUPPORTING EQUIPMENT

- A. Manufacturers:

1. ADEMCO Video; Pittway Corporation.
2. AXCESS Inc.
3. Crest Electronics, Inc.
4. General Electric.
5. Hitachi Visual Technologies.
6. JVC Professional Products.
7. Panasonic Security Systems Group.
8. Pelco.
9. Philips Communication, Security & Imaging; Philips Electronics N.V.
10. Safety Vision.
11. Samsung Opto-Electronics America, Inc.
12. SANYO Fisher Company; SANYO North America Corporation.
13. Sony.
14. Sensormatic Electronics Corporation.
15. Silent Witness Enterprises Ltd.
16. Toshiba Security Products.
17. Vicon Industries, Inc.

- B. Minimum Load Rating: Rated for load in excess of the total weight supported times a minimum safety factor of two.

- C. Mounting Brackets for Fixed Cameras: Type matched to items supported and mounting conditions. Include manual pan-and-tilt adjustment.
- D. 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. With sun shield that does 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 250, Type 3R.

2.9 MONITORS

- A. Available Manufacturers:
 - 1. ADEMCO Video; Pittway Corporation.
 - 2. AXCESS Inc.
 - 3. Crest Electronics, Inc.
 - 4. General Electric.
 - 5. Hitachi Visual Technologies.
 - 6. JVC Professional Products.
 - 7. Panasonic Security Systems Group.
 - 8. Pelco.
 - 9. Philips Communication, Security & Imaging; Philips Electronics N.V.
 - 10. Safety Vision.
 - 11. Samsung Opto-Electronics America, Inc.
 - 12. SANYO Fisher Company; SANYO North America Corporation.
 - 13. Sony.
 - 14. Sensormatic Electronics Corporation.
 - 15. Silent Witness Enterprises Ltd.
 - 16. Toshiba Security Products.
 - 17. Vicon Industries, Inc.
- B. Monochrome:
 - 1. Metal cabinet units designed for continuous operation.
 - 2. Screen Size (Diagonal Dimension): 13".
 - 3. Horizontal Resolution: 600 lines, minimum, at center.
 - 4. Minimum Front Panel Devices and Controls: Power switch, power-on indicator, and brightness, horizontal hold, vertical hold, and contrast controls.
 - 5. Mounting: Adjustable tilting and training.

6. Mounting: Single, 14-inch, vertical, EIA 19-inch (483-mm) electronic equipment rack or cabinet complying with EIA 310.
7. Electrical: 120-V ac, 60 Hz.

C. Color:

1. Video: 1-V peak to peak composite video, sync negative with loop through.
2. Screen Size (Diagonal Dimension): 19".
3. Resolution: 640 X 480 (NTSC)
4. Minimum Front Panel Devices and Controls: Power switch, power-on indicator, and brightness, contrast, color, and tint controls.
5. Degaussing: Automatic.
6. Mounting: Desk or wall bracket.
7. Electrical: 120-V ac, 60 Hz.

2.10 DIGITAL VIDEO RECORDERS

A. Manufacturers:

1. ADEMCO Video; Pittway Corporation.
2. AXCESS Inc.
3. Crest Electronics, Inc.
4. General Electric.
5. Hitachi Visual Technologies.
6. JVC Professional Products.
7. Panasonic Security Systems Group.
8. Pelco.
9. Philips Communication, Security & Imaging; Philips Electronics N.V.
10. Safety Vision.
11. Samsung Opto-Electronics America, Inc.
12. SANYO Fisher Company; SANYO North America Corporation.
13. Sony.
14. Sensormatic Electronics Corporation.
15. Silent Witness Enterprises Ltd.
16. Toshiba Security Products.
17. Vicon Industries, Inc.

B. Digital, time-lapse type, full frame and motion recorder, with removable hard drive.

1. Recording Rate: 120 image per second at 720 (H) X 240 (V) and 320 (H) X 240 (V) sampling.
2. Resolution: 720 by 480, minimum sampling and 3-D scan conversion for stabilized pictures in a single frame with five compression mode.
3. Programming shall be from trackball and push buttons on face of the recorder, settings shall be displayed on any video monitor connected to the recorder. Programming shall include the following:
 - a. Motion analysis graph.
 - b. Password protection.
 - c. Alarm and timer controls.
 - d. Continuous recording option.
 - e. Time-lapse operating modes.
 - f. Search video by time, event, or motion.

4. Programming: Smart Media card for software updating, image archiving, and image transfer to a PC.
 5. Storage: 250 GB removable IDE hard drive. Software shall permit hot-swapping drives.
 6. Time and Date Generator: Records time (hr:min:sec) and date legend of each frame.
 7. Audio Recording: 70 to 7000 Hz. Input: phono and microphone; output: photo.
 8. Mounting: Standard 19-inch rack complying with EIA 310, or freestanding desktop.
 9. 10/100 Base T connection for "record" review and "camera" view and control on a PC equipped with Microsoft Window XP professional operating system software and Microsoft Explorer internet browser software.
 10. Architecture shall allow multiple units to be cascaded in increments of 16 cameras. Include cascading function for the number of cameras on the project.
- C. Switcher: For displaying images from sixteen (16) cameras on a single monitor. Programmable switcher multiplexer shall be separate unit or shall be combined with DVR.
1. Camera functions and control shall be accessible for all cameras through the use of control units or matrix control system.
 2. Shall simultaneously permit direct camera selection for recording playback of any of 16 video sources, multi-screen viewing and multi-plexed camera encoding (triplex).
 3. Programmable switcher with dwell time and camera order programming. Unit shall automatically switch multiple camera images to enable sequential spot monitoring and simultaneous field recording. Unit shall provide separate spot, multi-screen, multi-screen/RGB and cascaded video monitor outputs. Unit shall offer full screen, 4, 7, 9, 10, 13 and 16 multi-screen monitoring modes.
 4. Unit shall furnish sixteen (16) looping vide outputs, four (4) channels of audio, one (1) external storage connection on external copy connection and two (2) independent video outputs assignable to multi-screen or spot functions.
 5. Shall be designed to rack mount, 120 VAC per module.
- D. Camera Controls: Arranged for multiple-camera control, with switches to select camera to be controlled.
1. Camera Control: 3D joystick type, single hand control of pan, tilt and zoom function of PTZ camera.
 2. Recorder Control: Jog dial and shuttling to find disk recorder book marks and input others settings, separate buttons for playback, recording and search function.
 3. Switcher Control: Control for fully array of image switching/sequencing and display position camera title on/off.
 4. User setting button.
 5. Program upload function.
- 2.11 VIDEO MOTION SENSORS (INTERIOR)
- A. Available Manufacturers:
1. A & S Security Products, Inc.
 2. AXCESS Inc.
 3. ICU Security, Inc.
 4. Sensormatic Electronics Corporation.
 5. Visiontech.
- B. Device Performance: Detect changes in video signal within a user-defined protected zone. Video inputs shall be composite video as defined in SMPTE 170. Provide an alarm output for each video input.

1. Detect movement within protected zone of intruders wearing clothing with a reflectivity that differs from that of background scene by a factor of two. Reject all other changes in video signal.
2. Modular design that allows for expansion or modification of number of inputs.
3. Controls:
 - a. Size of detection zones.
 - b. Sensitivity of detection of each protected zone.
4. Mounting: Standard 19-inch rack complying with EIA 310.

2.12 CONTROL STATIONS

- A. Power Continuity for Control Station: Batteries in power supplies of central-station control units and individual system components shall maintain continuous system operation during outages of both normal and backup ac system supply.
 1. Batteries: Rechargeable, valve-regulated, recombinant, sealed, lead-acid type with nominal 10-year life expectancy. Capacity adequate to operate portion of system served, including audible trouble signal devices for up to 4 hours and audible and visual alarm devices under alarm conditions for an additional 10 minutes.
 2. Battery Charger: Solid-state, fully automatic, variable-charging-rate type. Charger shall recharge fully discharged battery within 24 hours.
- B. Annunciation: Indicate a change in system condition and switching of system or component to backup power.

2.13 SIGNAL TRANSMISSION COMPONENTS

- A. Cable: Coaxial cable elements have 75-ohms nominal impedance. Cables shall comply with Division 27 Section "Master Antenna Television System" and shall be composite cable which includes BNC type, 75 ohms, and 2-conductor, 18 awg for power. Category 6 shall comply with Division 27 Section "Communications Horizontal Cabling".
- B. Video Surveillance Coaxial Cable Connectors: BNC type, 75 ohms. Of three-piece construction, consisting of a crimp-type center tip, sleeve, and main body.

PART 3 - EXECUTION

3.1 WIRING

- A. Wiring Method: Install cables in raceways and as otherwise indicated. Conceal raceways and wiring except in unfinished spaces.
- B. Wiring within Enclosures: Bundle, lace, and train conductors to terminal points with no excess and without exceeding manufacturer's limitations on bending radii. Provide and use lacing bars and distribution spools.
- C. Splices, Taps, and Terminations: For power and control wiring, use numbered terminal strips in junction, pull, and outlet boxes; terminal cabinets; and equipment enclosures. Tighten electrical

connectors and terminals according to manufacturer's published torque-tightening values. If manufacturer's torque values are not indicated, use those specified in UL 486A and UL 486B.

- D. Grounding: Provide independent-signal circuit grounding recommended in writing by manufacturer.

3.2 VIDEO SURVEILLANCE SYSTEM INSTALLATION

- A. Install cameras and infrared illuminators level and plumb.
- B. Install cameras with 84-inch minimum clear space below cameras and their mountings. Change type of mounting to achieve required clearance.
- C. Set pan-and-tilt unit stops to suit final camera position and to obtain the field of view required for camera. Connect all controls and alarms and adjust.
- D. Install power supplies and other auxiliary components at control stations, unless otherwise indicated.
- E. Install tamper switches on components indicated to receive tamper switches, arranged to detect unauthorized entry into system component enclosures, and mounted in self-protected, inconspicuous positions.
- F. Avoid ground loops by making ground connections at only the control station.
 - 1. For 12- and 24-V dc cameras, connect the coaxial cable shields only at the monitor end.
- G. Identify system components, wiring, cabling, and terminals according to Division 26 Section "Identification of Electrical Systems."

3.3 FIELD QUALITY CONTROL

- A. Manufacturer's Field Service: Engage a factory-authorized service representative to inspect field-assembled components and equipment installation and supervise pretesting, testing, and adjusting of video surveillance equipment.
- B. Inspection: Verify that units and controls are properly installed, connected, and labeled, and that interconnecting wires and terminals are identified.
- C. Pretesting: Align and adjust system and pretest components, wiring, and functions to verify that they comply with specified requirements. Conduct tests at varying lighting levels, including day and night scenes as applicable. Prepare video surveillance equipment for acceptance and operational testing as follows:
 - 1. Prepare equipment list described in Part 1 "Submittals" Article.
 - 2. Verify operation of auto-iris lenses.
 - 3. Set back-focus of fixed focal length lenses. At focus set to infinity, simulate nighttime lighting conditions by using a dark glass filter of a density that produces a clear image. Adjust until image is in focus with and without the filter.
 - 4. Set back-focus of zoom lenses. At focus set to infinity, simulate nighttime lighting conditions by using a dark glass filter of a density that produces a clear image. Additionally, set zoom to full wide angle and aim camera at an object 50 to 75 feet away. Adjust until image is in focus from full wide angle to full telephoto, with the filter in place.

5. Set and name all preset positions; consult Owner's personnel.
 6. Set sensitivity of motion detection.
 7. Connect and verify responses to alarms.
 8. Verify operation of control-station equipment.
- D. Test Schedule: Schedule tests after pretesting has been successfully completed and system has been in normal functional operation for at least 14 days. Provide a minimum of 10 days' notice of test schedule.
- E. Operational Tests: Perform operational system tests to verify that system complies with Specifications. Include all modes of system operation. Test equipment for proper operation in all functional modes.
- F. Remove and replace malfunctioning items and retest as specified above.
- G. Record test results for each piece of equipment.
- H. Retest: Correct deficiencies identified by tests and observations and retest until specified requirements are met.

3.4 ADJUSTING

- A. Occupancy Adjustments: When requested within 12 months of date of Substantial Completion, provide on-site assistance in adjusting system to suit actual occupied conditions and to optimize performance of the installed equipment. Tasks shall include, but are not limited to, the following:
1. Check cable connections.
 2. Check proper operation of cameras and lenses. Verify operation of auto-iris lenses and adjust back-focus as needed.
 3. Adjust all preset positions; consult Owner's personnel.
 4. Recommend changes to cameras, lenses, and associated equipment to improve Owner' utilization of video surveillance system.
 5. Provide a written report of adjustments and recommendations.

3.5 CLEANING

- A. Clean installed items using methods and materials recommended in writing by manufacturer.
- B. Clean video surveillance system components, including camera-housing windows, lenses, and monitor screens.

3.6 DEMONSTRATION

- A. Engage a factory-authorized service representative to train Owner's maintenance personnel to adjust, operate, and maintain video surveillance equipment.
1. Train Owner's maintenance personnel on procedures and schedules for troubleshooting, servicing, and maintaining equipment.
 2. Demonstrate methods of determining optimum alignment and adjustment of components and settings for system controls.

3. Review equipment list and data in maintenance manuals. Refer to Division 01 Section "Operation and Maintenance Data"
4. Conduct a minimum of four hours' training as specified in instructions to Owner's employees in Division 01 Section "Demonstration and Training"

END OF SECTION 28 23 00

SECTION 28 31 11
DIGITAL, ADDRESSABLE FIRE-ALARM SYSTEM

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. Fire-alarm control unit.
 - 2. Manual fire-alarm boxes.
 - 3. System smoke detectors.
 - 4. Heat detectors.
 - 5. Notification appliances.
 - 6. Addressable interface device.
 - 7. Digital alarm communicator transmitter.
 - 8. System printer.

1.3 DEFINITIONS

- A. LED: Light-emitting diode.
- B. NICET: National Institute for Certification in Engineering Technologies.
- C. FACP: Fire Alarm Control Panel.
- D. FANP: Fire Alarm Power Extender Panel.
- E. FAAP: Fire Alarm Annunciator (LCD).

1.4 SYSTEM DESCRIPTION

- A. Non-coded, UL-certified addressable system, with multiplexed signal transmission, dedicated to fire-alarm service only.
- B. Comply with NFPA 72.

1.5 SUBMITTALS

- A. General Submittal Requirements:
 - 1. Submittals shall be approved by authorities having jurisdiction prior to submitting them to Architect.

2. Shop Drawings shall be prepared by persons with the following qualifications:
 - a. Licensed or certified by authorities having jurisdiction.
- B. Product Data: For each type of product indicated.
- C. Shop Drawings: For fire-alarm system. Include plans, elevations, sections, details, and attachments to other work.
 1. Comply with recommendations in the "Documentation" Section of the "Fundamentals of Fire Alarm Systems" Chapter in NFPA 72.
 2. Include voltage drop calculations for notification appliance circuits.
 3. Include battery-size calculations.
 4. Include performance parameters and installation details for each detector, verifying that each detector is listed for complete range of air velocity, temperature, and humidity possible when air-handling system is operating.
 5. Include plans, sections, and elevations of heating, ventilating, and air-conditioning ducts, drawn to scale and coordinating installation of duct smoke detectors and access to them. Show critical dimensions that relate to placement and support of sampling tubes, detector housing, and remote status and alarm indicators. Locate detectors according to manufacturer's written recommendations.
 6. Include voice/alarm signaling-service equipment rack or console layout, grounding schematic, amplifier power calculation, and single-line connection diagram.
 7. Include floor plans to indicate final outlet locations showing address of each addressable device. Show size and route of cable and conduits.
- D. Qualification Data: For qualified Installer.
- E. Field quality-control reports.
- F. Operation and Maintenance Data: For fire-alarm systems 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. Comply with the "Records" Section of the "Inspection, Testing and Maintenance" Chapter in NFPA 72.
 2. Provide "Record of Completion Documents" according to NFPA 72 article "Permanent Records" in the "Records" Section of the "Inspection, Testing and Maintenance" Chapter.
 3. Record copy of site-specific software.
 4. Provide "Maintenance, Inspection and Testing Records" according to NFPA 72 article of the same name and include the following:
 - a. Frequency of testing of installed components.
 - b. Frequency of inspection of installed components.
 - c. Requirements and recommendations related to results of maintenance.
 - d. Manufacturer's user training manuals.
 5. Manufacturer's required maintenance related to system warranty requirements.
 6. Abbreviated operating instructions for mounting at fire-alarm control unit.
- G. Software and Firmware Operational Documentation:
 1. Software operating and upgrade manuals.
 2. Program Software Backup: CD disk, complete with data files.
 3. Device address list.

4. Printout of software application and graphic screens.

1.6 QUALITY ASSURANCE

- A. Installer Qualifications: Personnel shall be trained and certified by manufacturer for installation of units required for this Project.
- B. Installer Qualifications: Installation shall be by personnel certified by NICET as fire-alarm Level II technician.
- C. Source Limitations for Fire-Alarm System and Components: Obtain fire-alarm system from single source from single manufacturer.
- 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.

1.7 SOFTWARE SERVICE AGREEMENT

- A. Comply with UL 864.
- B. Technical Support: Beginning with Substantial Completion, provide software support for two years.
- C. 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.

1.8 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. Lamps for Remote Indicating Lamp Units: Quantity equal to 10 percent of amount installed, but no fewer than 1 unit.
 2. Lamps for Strobe Units: Quantity equal to 10 percent of amount installed, but no fewer than 1 unit.
 3. Smoke Detectors: Quantity equal to 10 percent of amount of each type installed, but no fewer than 1 unit of each type.
 4. Detector Bases: Quantity equal to 2 percent of amount of each type installed, but no fewer than 1 unit of each type.
 5. Keys and Tools: One extra set for access to locked and tamper-proofed components.
 6. Audible and Visual Notification Appliances: One of each type installed.
 7. Fuses: Two of each type installed in the system.

1.9 WARRANTY

- A. Written warranty, executed by manufacturer agency to repair or replace equipment, devices, and auxiliary components that fail in material or workmanship within specified warranty period.

1. Warranty Period: Two years from the date of substantial completion.

PART 2 - PRODUCTS

2.1 MANUFACTURERS

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

1. General Electric Company/EST.
2. NOTIFIER; a Honeywell company.
3. Siemens Building Technologies, Inc.; Fire Safety Division.

2.2 SYSTEMS OPERATIONAL DESCRIPTION

- A. Fire-alarm signal initiation shall be by one or more of the following devices and systems:

1. Manual stations.
2. Verified automatic alarm operation of smoke detectors.
3. Automatic sprinkler system water flow.

- B. Fire-alarm signal shall initiate the following actions:

1. Continuously operate alarm notification appliances.
2. Identify alarm at fire-alarm control unit FACP.
3. Transmit an alarm signal to the remote alarm receiving station.
4. Unlock electric door locks in designated egress paths.
5. Release fire and smoke doors held open by magnetic door holders.
6. Activate voice/alarm communication system.
7. Switch heating, ventilating, and air-conditioning equipment controls to fire-alarm mode.
8. Activate emergency shutoffs for gas and fuel supplies.
9. Record events in the system memory.
10. Record events by the system printer.

- C. Supervisory signal initiation shall be by one or more of the following devices and actions:

1. Valve supervisory switch.

- D. System trouble signal initiation shall be by one or more of the following devices and actions:

1. Open circuits, shorts, and grounds in designated circuits.
2. Opening, tampering with, or removing alarm-initiating and supervisory signal-initiating devices.
3. Loss of primary power at fire-alarm control unit FACP.
4. Ground or a single break in fire-alarm control unit internal circuits.
5. Abnormal ac voltage at fire-alarm control unit FACP.
6. Break in standby battery circuitry.

7. Failure of battery charging.
 8. Abnormal position of any switch at fire-alarm control unit FACP.
 9. Removal of an alarm initiating device.
- E. System Trouble and Supervisory Signal Actions: Initiate notification appliance and annunciate at fire-alarm control unit FACP. Record the event on system printer.

2.3 FIRE-ALARM CONTROL UNIT

A. General Requirements for Fire-Alarm Control Unit:

1. Enclosure: Steel, baked enamel, painted cabinet with indicator viewing window, removable hinged outer door with cylinder lock and dead front construction with the outer door open. The inner dead front doors shall be hinged for ease of system operation by firefighters and access by technicians for testing and maintenance modes.
2. Field-programmable, microprocessor-based, modular, power-limited design with electronic modules, complying with UL 864 and listed and labeled by an NRTL.
 - a. 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.
 - b. 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.
 - a. Smoke sensors shall additionally communicate sensitivity setting and allow for adjustment of sensitivity at fire-alarm control unit.
 - b. Temperature sensors shall additionally test for and communicate the sensitivity range of the device.
4. Addressable control circuits for operation of mechanical equipment.
5. Digital communication capabilities supporting Style 4 (Class B) communications using DC digital and fiber optics technologies as required for the control panel to communicate with network nodes including remote fire alarm panels, interface with building automation system, graphic command center, remote annunciators and displays, both global displaying total network information.
 - a. Capability shall exist within the system to extend the network at any node. The system shall support a maximum of two network extension circuits in series on any system branch, extending the inherent distance limitations for network communications.
 - b. Communication protocol shall be of the CS/MACD (carrier sense, multiple access, collision detect) type, RJ-485 token ring configuration or "ARNET" communication protocol.
6. The system shall have built-in equipment allowing reporting of system events to pagers.
7. The system shall employ a RS-232 RS485, TCP/IP and other interface protocol to interface with building automation system.

- B. Alphanumeric Display and System Controls: Arranged for interface between human operator at fire-alarm 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: Liquid-crystal type, 3 line(s) of 80 characters, minimum.
 2. Keypad: Arranged to permit entry and execution of programming, display, and control commands.
- C. Circuits:
1. Initiating Device, Notification Appliance, and Signaling Line Circuits:
 - a. Initiating Device Circuits NFPA 72, Class A.
 - b. Notification Appliance Circuits: Class B.
 - c. Signaling Line Circuits: Style 6.
 2. Initiating Device, Notification Appliance, and Signaling Line Circuits:
 - a. Initiating Device Circuits NFPA 72, Class B.
 - b. Notification Appliance Circuits Class B.
 - c. Signaling Line Circuits: Style 4.
 3. Serial Interfaces: Two RS-232 ports for printers.
- D. Smoke-Alarm Verification:
1. Initiate audible and visible indication of an "alarm-verification" signal at fire-alarm control unit.
 2. Activate an approved "alarm-verification" sequence at fire-alarm control unit and detector.
 3. Record events by the system printer.
 4. Sound general alarm if the alarm is verified.
 5. Cancel fire-alarm control unit indication and system reset if the alarm is not verified.
- E. Door Controls: Door hold-open devices that are controlled by smoke detectors at doors in walls shall be connected to fire-alarm system.
- F. Remote Smoke-Detector Sensitivity Adjustment: Controls shall select specific addressable smoke detectors for adjustment, display their current status and sensitivity settings, and change those settings. Allow controls to be used to program repetitive, time-scheduled, and automated changes in sensitivity of specific detector groups. Record sensitivity adjustments and sensitivity-adjustment schedule changes in system memory, and print out the final adjusted values on system printer.
- G. Transmission to Remote Alarm Receiving Station: Automatically transmit alarm, supervisory, and trouble signals to a remote alarm station.
- H. Voice/Alarm Signaling Service: Central emergency communication system with redundant microphones, preamplifiers, amplifiers, and tone generators provided as a special module that is part of fire-alarm control unit.
1. Indicated number of alarm channels for automatic, simultaneous transmission of different announcements to different zones or for manual transmission of announcements by use of the central-control microphone. Amplifiers shall comply with UL 1711 and be listed by an NRTL.
 - a. Allow the application of and evacuation signal to indicated number of zones and, at same time, allow voice paging to the other zones selectively or in any combination.
 - b. Programmable tone and message sequence selection.
 - c. Standard digitally recorded messages for "Evacuation" and "All Clear."

- d. Generate tones to be sequenced with audio messages of type recommended by NFPA 72 and that are compatible with tone patterns of notification appliance circuits of fire-alarm control unit.
- 2. Status Annunciator: Indicate the status of various voice/alarm speaker zones and the status of firefighters' two-way telephone communication zones.
- 3. Preamplifiers, amplifiers, and tone generators shall automatically transfer to backup units, on primary equipment failure.
- I. 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.
- J. Primary Power: 24-V dc obtained from 120-V ac service and a power-supply module. Initiating devices, notification appliances, signaling lines, trouble signals, supervisory and digital alarm communicator transmitters shall be powered by 24-V dc source.
 - 1. Alarm current draw of entire fire-alarm system shall not exceed 80 percent of the power-supply module rating.
- K. Secondary Power: 24-V dc supply system with batteries, automatic battery charger, and automatic transfer switch.
 - 1. Batteries: Sealed lead calcium.
- L. Instructions: Computer printout or typewritten instruction card mounted behind a plastic or glass cover in a stainless-steel or aluminum frame. Include interpretation and describe appropriate response for displays and signals. Briefly describe the functional operation of the system under normal, alarm, and trouble conditions.

2.4 MANUAL FIRE-ALARM BOXES

- A. General Requirements for Manual Fire-Alarm Boxes: Comply with UL 38. Boxes shall be finished in red with molded, raised-letter operating instructions in contrasting color; shall show visible indication of operation; and shall be mounted on recessed outlet box. If indicated as surface mounted, provide manufacturer's surface back box.
 - 1. Double-action mechanism requiring two actions to initiate an alarm, pull-lever type; with integral addressable module arranged to communicate manual-station status (normal, alarm, or trouble) to fire-alarm control unit FACP.
 - 2. Station Reset: Key- or wrench-operated switch.
 - 3. Indoor Protective Shield: Factory-fabricated clear plastic enclosure hinged at the top to permit lifting for access to initiate an alarm. Lifting the cover actuates an integral battery-powered audible horn intended to discourage false-alarm operation.

2.5 SYSTEM SMOKE DETECTORS

- A. Multi-Sensor Type System Smoke Detectors:

1. Comply with UL 268; operating at 24-V dc, nominal, multi-sensor type containing photoelectrical sensor, tested according to UL 268A and thermal sensor, combination of rate of rise and fixed temperature.
 2. Integral Addressable Module: Arranged to communicate detector status (normal, alarm, or trouble) to fire-alarm control unit **FACP**.
 3. Base Mounting: Detector shall be mounted in a twist-lock module that connects to a fixed base. Provide terminals in the fixed base for connection to building wiring.
 4. Self-Restoring: Detectors do not require resetting or readjustment after actuation to restore them to normal operation.
 5. Integral Visual-Indicating Light: LED type indicating detector has operated and power-on status.
- B. Duct Smoke Detectors: Photoelectric type complying with UL 268A and specified above.
1. Weatherproof Duct Housing Enclosure: NEMA 250, Type 4X; NRTL listed for use with the supplied detector.
 2. Each sensor shall have multiple levels of detection sensitivity.
 3. Sampling Tubes: Design and dimensions as recommended by manufacturer for specific duct size, air velocity, and installation conditions where applied.
 4. Relay Fan Shutdown: Rated to interrupt fan motor-control circuit.
- C. Heat Detectors:
1. General Requirements for Heat Detectors: Comply with UL 521.
 2. Heat Detector, Combination Type: Comply with UL 521. Actuated by either a fixed temperature of 135 deg. F or a rate of rise that exceeds 15 deg F per minute unless otherwise indicated.
 3. Mounting: Twist-lock base interchangeable with smoke-detector bases.
 4. Integral Addressable Module: Arranged to communicate detector status (normal, alarm, or trouble) to fire-alarm control unit.
 5. Mounting: Twist-lock base interchangeable with smoke-detector bases.
 6. Integral Addressable Module: Arranged to communicate detector status (normal, alarm, or trouble) to fire-alarm control unit.

2.6 NOTIFICATION APPLIANCES

- A. General Requirements for Notification Appliances: Individually addressed, connected to a signaling line circuit (zoned as indicated), equipped for mounting as indicated and with screw terminals for system connections.
- B. Horns: Electronic type, 24-V dc; with provision for housing the operating mechanism behind a grille. Comply with UL 464. Horns shall produce a sound-pressure level of **[Insert Option Here]** dBA, measured 10 feet from the horn, using the coded signal prescribed in UL 464 test protocol, minimum ten (10) selectable tone.
- C. Voice/Tone Notification Appliances:
1. Appliances shall comply with UL 1480 and shall be listed and labeled by an NRTL.
 2. High-Range Units: Rated 2 to 15 W Mech/Equipment Room.
 3. Low-Range Units: Rated 1 to 2 W.
 4. Mounting: Semi-recessed.
 5. Matching Transformers: Tap range matched to acoustical environment of speaker location.

- D. Visible Notification Appliances: Xenon strobe lights comply with UL 1971, with clear or nominal white polycarbonate lens mounted on an aluminum faceplate. The word "FIRE" is engraved in minimum 1-inch high letters on the lens.
1. Rated Light Output: 15/30/75/110 cd, selectable in the field.
 2. Mounting: Wall mounted unless otherwise indicated.
 3. For units with guards to prevent physical damage, light output ratings shall be determined with guards in place.
 4. Flashing shall be in a temporal pattern, synchronized with other units.
 5. Strobe Leads: Factory connected to screw terminals.
 6. Mounting Faceplate: Factory finished, white.

2.7 MAGNETIC DOOR HOLDERS

- A. Description: Units are equipped for wall or floor mounting as indicated and are complete with matching doorplate.
1. Electromagnet: Requires no more than 3 W to develop 25-lbf holding force.
 2. Wall-Mounted Units: Flush mounted unless otherwise indicated.
 3. Rating: 24-V ac or dc.
- B. Material and Finish: Match door hardware.

2.8 ADDRESSABLE INTERFACE DEVICE

- A. Description: Microelectronic monitor module, NRTL listed for use in providing a system address for alarm-initiating devices for wired applications with normally open contacts.

2.9 DIGITAL ALARM COMMUNICATOR TRANSMITTER

- A. Digital alarm communicator transmitter shall be acceptable to the remote central station and shall comply with UL 632.
- B. Local functions and display at the digital alarm communicator transmitter shall include the following:
1. Verification that both telephone lines are available.
 2. Programming device.
 3. LED display.
 4. Manual test report function and manual transmission clear indication.
 5. Communications failure with the central station or fire-alarm control unit.
- C. Digital data transmission shall include the following:
1. Address of the alarm-initiating device.
 2. Address of the supervisory signal.
 3. Address of the trouble-initiating device.
 4. Loss of ac supply or loss of power.
 5. Low battery.
 6. Abnormal test signal.
 7. Communication bus failure.

- D. Secondary Power: Integral rechargeable battery and automatic charger.
- E. Self-Test: Conducted automatically every 24 hours with report transmitted to central station.

2.10 RADIO ALARM TRANSMITTER

- A. Transmitter shall comply with NFPA 1221 and shall be listed and labeled by an NRTL.
- B. Comply with 47 CFR 90.
- C. Description: Manufacturer's standard commercial product; factory assembled, wired, tested, and ready for installation and operation.
 - 1. Packaging: A single, modular, NEMA 250, Type 1 metal enclosure with a tamper-resistant flush tumbler lock.
 - 2. Signal Transmission Mode and Frequency: VHF or UHF 2-W power output, coordinated with operating characteristics of the established remote alarm receiving station designated by Owner.
 - 3. Normal Power Input: 120-V ac.
 - 4. Secondary Power: Integral-sealed, rechargeable, 12-V battery and charger. Comply with NFPA 72 requirements for battery capacity; submit calculations.
 - 5. Antenna: Omni-directional, coaxial half-wave, dipole type with driving point impedance matched to transmitter and antenna cable output impedance. Wind-load strength of antenna and mounting hardware and supports shall withstand 100 mph with a gust factor of 1.3 without failure.
 - 6. Antenna Cable: Coaxial cable with impedance matched to the transmitter output impedance.
 - 7. Antenna-Cable Connectors: Weatherproof.
 - 8. Alarm Interface Devices: Circuit boards, modules, and other auxiliary devices, integral to the transmitter, matching fire-alarm and other system outputs to message-generating inputs of the transmitter that produce required message transmissions.
- D. Functional Performance: Unit shall receive an alarm, supervisory, or trouble signal from fire-alarm control unit or from its own internal sensors or controls and shall automatically transmit signal along with a unique code that identifies the transmitting station to the remote alarm receiving station. Transmitted messages shall correspond to standard designations for fire-reporting system to which the signal is being transmitted and shall include separately designated messages in response to the following events or conditions:
 - 1. Transmitter Low-Battery Condition: Sent when battery voltage is below 85 percent of rated value.
 - 2. System Test Message: Initiated manually by a test switch within the transmitter cabinet, or automatically at an optionally preselected time, once every 24 hours, with transmission time controlled by a programmed timing device integral to transmitter controls.
 - 3. Transmitter Trouble Message: Actuated by failure, in excess of one-minute duration, of the transmitter normal power source, derangement of the wiring of the transmitter, or any alarm input interface circuit or device connected to it.
 - 4. Local Fire-Alarm-System Trouble Message: Initiated by events or conditions that cause a trouble signal to be indicated on the building system.
 - 5. Local Fire-Alarm-System Alarm Message: Actuated when the building system goes into an alarm state. Identifies device that initiated the alarm.
 - 6. Local Fire-Alarm-System Supervisory-Alarm Message: Actuated when the building alarm system indicates a supervisory alarm.

2.11 SYSTEM PRINTER

- A. Printer shall be listed and labeled by an NRTL as an integral part of fire-alarm system.

2.12 WIRE AND CABLE

- A. Wire and cable for fire alarm systems shall be UL listed and labeled as complying with NFPA 70, Article 760.
- B. Signaling Line Circuits: Twisted, shielded pair, not less than No. 18 AWG or size as recommended by system manufacturer.
- C. Non-Power-Limited Circuits: Solid-copper conductors with 600-V rated, 75 deg C, color-coded insulation.
 - 1. Low-Voltage Circuits: No. 18 AWG, minimum and recommended by system supplier.
 - 2. Line-Voltage Circuits: No. 12 AWG, minimum and recommended by system supplier.
- D. Multi-conductor Armored Cable: NFPA 70 Type MC, copper conductors, TFN/THHN conductor insulation, copper drain wire, armor with outer jacket with red identifier stripe, UL listed for fire alarm and cable tray installation, plenum rated and size/pair, recommended by system supplier.

PART 3 - EXECUTION

3.1 EQUIPMENT INSTALLATION

- A. Comply with NFPA 72 for installation of fire-alarm equipment.
- B. Equipment Mounting: Install fire-alarm control unit on finished floor with tops of cabinets not more than 72 inches (1830 mm) above the finished floor.
- C. Detector Spacing:
 - 1. Comply with NFPA 72, "Smoke-Sensing Fire Detectors" Section in the "Initiating Devices" Chapter, for smoke-detector spacing and shown on Contract Documents.
 - 2. Smooth ceiling spacing shall not exceed 30 feet.
 - 3. Spacing of detectors for irregular areas, for irregular ceiling construction, and for high ceiling areas shall be determined according to Appendix A in NFPA 72.
 - 4. HVAC: Locate detectors not closer than 5 feet from air-supply diffuser or return-air opening.
 - 5. Lighting Fixtures: Locate detectors not closer than 12 inches from any part of a lighting fixture.
- D. Duct Smoke Detectors: Comply with NFPA 72 and NFPA 90A. Install sampling tubes so they extend the full width of duct.
- E. Remote Status and Alarm Indicators: Install near each smoke detector and each sprinkler water-flow switch and valve-tamper switch that is not readily visible from normal viewing position.
- F. Indicating Devices: Install at 80" A.F.F. to center.
- G. Manual Pull Station: Install at 48" A.F.F. to center.

- H. Device Location-Indicating Lights: Locate in public space (in ceiling) near the device they monitor.
- I. Fire-Alarm Control Unit: Surface mounted, with tops of cabinets not more than 72 inches above the finished floor.
- J. Antenna for Radio Alarm Transmitter: Mount to building structure where indicated. Use mounting arrangement and substrate connection that will resist 100-mph wind load with a gust factor of 1.3 without damage.

3.2 CONNECTIONS

- A. For fire-protection systems related to doors in fire-rated walls and partitions and to doors in smoke partitions, comply with requirements in Division 08 Section "Door Hardware." Connect hardware and devices to fire-alarm system.
 - 1. Verify that hardware and devices are NRTL listed for use with fire-alarm system in this Section before making connections.
- B. Make addressable connections with a supervised interface device to the following devices and systems. Install the interface device less than 3 feet from the device controlled. Make an addressable confirmation connection when such feedback is available at the device or system being controlled.
 - 1. Smoke dampers in air ducts of designated air-conditioning duct systems.
 - 2. Alarm-initiating connection to activate emergency shutoffs for gas and fuel supplies.
 - 3. Supervisory connections at valve supervisory switches.

3.3 IDENTIFICATION

- A. Identify system components, wiring, cabling, and terminals. Comply with requirements for identification specified in Division 26 Section "Identification for Electrical Systems."
- B. Install framed instructions in a location visible from fire-alarm control unit.
- C. Install device address at each device.

3.4 GROUNDING

- A. Ground fire-alarm control unit and associated circuits; comply with IEEE 1100. Install a ground wire from main service ground to fire-alarm control unit.

3.5 FIELD QUALITY CONTROL

- A. Field tests shall be witnessed by authorities having jurisdiction.
- B. 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.

C. Tests and Inspections:

1. Visual Inspection: Conduct visual inspection prior to testing.
 - a. Inspection shall be based on completed Record Drawings and system documentation that is required by NFPA 72 in its "Completion Documents, Preparation" Table in the "Documentation" Section of the "Fundamentals of Fire Alarm Systems" Chapter.
 - b. Comply with "Visual Inspection Frequencies" Table in the "Inspection" Section of the "Inspection, Testing and Maintenance" Chapter in NFPA 72; retain the "Initial/Reacceptance" column and list only the installed components.
2. System Testing: Comply with "Test Methods" Table in the "Testing" Section of the "Inspection, Testing and Maintenance" Chapter in NFPA 72.
3. Test audible appliances for the public operating mode according to manufacturer's written instructions. Perform the test using a portable sound-level meter complying with Type 2 requirements in ANSI S1.4.
4. Test audible appliances for the private operating mode according to manufacturer's written instructions.
5. Test visible appliances for the public operating mode according to manufacturer's written instructions.
6. Factory-authorized service representative shall prepare the "Fire Alarm System Record of Completion" in the "Documentation" Section of the "Fundamentals of Fire Alarm Systems" Chapter in NFPA 72 and the "Inspection and Testing Form" in the "Records" Section of the "Inspection, Testing and Maintenance" Chapter in NFPA 72.

D. Reacceptance Testing: Perform reacceptance testing to verify the proper operation of added or replaced devices and appliances.

E. Fire-alarm system will be considered defective if it does not pass tests and inspections.

F. Prepare test and inspection reports.

3.6 DEMONSTRATION

- A. Engage a factory-authorized service representative to train Owner's maintenance personnel to adjust, operate, and maintain fire-alarm system.

END OF SECTION 28 31 11