

**SECTION 28 13 00**  
**ACCESS CONTROL**

**PART 1 - GENERAL**

**1.1 RELATED DOCUMENTS DEFINITIONS**

- 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. This Section includes additions of access controlled doors to the existing campus security access control system (Johnson Controls CardKey) consisting of campus networked controllers already existing in the buildings to receive the new access controlled doors. In general, new two-door controller modules and/or panels that interface with the existing controller panels shall be installed and the main operating system software shall be programmed to accept these new doors into the system.

**1.3 DEFINITIONS**

- A. Controller: An intelligent peripheral control unit that uses a computer for controlling its operation.
- B. CPU: Central processing unit.
- C. Credential: Data assigned to an entity and used to identify that entity.
- D. 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.
- E. I/O: Input/Output.
- F. LAN: Local area network.
- G. LED: Light-emitting diode.
- H. Location: A Location on the network having a Controller-to-Controller communications link, with additional Controllers connected with RS-485 communications loop.
- I. RS-485: An TIA/EIA standard for multipoint communications.
- J. TCP/IP: Transport control protocol/Internet protocol incorporated into Microsoft Windows.

- K. UPS: Uninterruptible power supply.
- L. Wiegand: Patented magnetic principle that uses specially treated wires embedded in the credential card.

#### **1.4 SYSTEM DESCRIPTION**

- A. System shall consist of a connection to a campus networked system and field-installed Controllers, connected by a high-speed electronic data transmission network.
  - 1. System Software: Existing Johnson Controls CardKey P2000 control system software.

#### **1.5 PERFORMANCE REQUIREMENTS**

Security access system shall use the existing single database for access-control and credential-creation functions. Field equipment shall include new door controller modules and/or panels, door contact switches, motion detectors, and proximity card readers. The new controller boards shall serve as an interface between the campus system and door devices.

- A. System Response to Alarms: Field device network shall provide a system alarm to be annunciated at the Central Station for two door functions: Forced entry and/or propped open door.
- B. 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. Reader assemblies.
  - b. Controller module/panel to door devices.
  - c. New panel connections to existing panels.
4. Cable Administration Drawings: As specified in Part 3 "Identification" Article.
5. Battery and charger calculations for Controllers.
- C. Field quality-control test reports.
- D. Operation and Maintenance Data: For security system to include in emergency, operation, and maintenance manuals.

#### **1.7 QUALITY ASSURANCE**

- A. Installer Qualifications: An employer of workers trained and approved by manufacturer.
- B. Testing Agency Qualifications: An independent agency, with the experience and capability to conduct the testing indicated, that is a nationally recognized testing laboratory (NRTL) as defined by OSHA in 29 CFR 1910.7, and that is acceptable to authorities having jurisdiction.
- C. Source Limitations: Obtain controllers, card readers, and all software through one source from a single manufacturer.
- D. 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.
- E. Comply with NFPA 70, "National Electrical Code."
- F. Comply with SIA DC-01 and SIA DC-03.

#### **1.8 DELIVERY, STORAGE, AND HANDLING**

- A. Controllers:
  1. Store in temperature and humidity-controlled environment in original manufacturer's sealed containers. Maintain ambient temperature between 50 and 85 deg F (10 and 30 deg C), and not more than 80 percent relative humidity, noncondensing.
  2. Open each container; verify contents against packing list, and file copy of packing list, complete with container identification for inclusion in operation and maintenance data.

3. Mark packing list with 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 geographic environmental conditions without mechanical or electrical damage or degradation of operating capability.

### **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 the manufacturers specified.

#### **2.2 SECURITY ACCESS SYSTEM**

- A. Manufacturer:
  1. Johnson Controls CardKey
- B. Controller Software:
  1. Compatible with the existing P2000 system software.

#### **2.3 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.

#### **2.4 SURGE AND TAMPER PROTECTION**

- A. Surge Protection: Protect components from voltage surges originating external to equipment housing and entering through power, communication, signal, control, or sensing leads. Include surge protection for external wiring of each conductor-entry connection to components.
  1. Minimum Protection for Power Connections 120 V and More:  
Auxiliary panel suppressors complying with requirements in Division 26 Section "Transient-Voltage Suppression for Low-Voltage Electrical Power Circuits."

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

## **2.5 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 20 minutes, complying with UL 924.

## **2.6 CARD READERS**

- A. Power: Card reader shall be powered from its associated Controller, including its standby power source.
- B. Mounting: Card reader shall be "mullion" style and installed to the door frame.

## **2.7 DOOR HARDWARE INTERFACE**

- A. Electric Door Locksets (Double Doors): Signal switches shall transmit data to Controller to indicate when "request to exit" function is to be activated. Power and signal shall be from the Controller. Electric locksets are specified in Division 08 "Door Hardware."
- B. Electric Strikes (Single Doors): Power shall be from the Controller. Electric strikes are specified in Division 08 "Door Hardware."

## **2.8 CABLES**

- A. Manufacturers:
  1. Belden Inc.; Electronics Division.
  2. CommScope.
  3. Mohawk/CDT; a division of Cable Design Technologies.
  4. 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. RS-485 communications require 2 twisted pairs, with a distance limitation of 4000 feet.
- D. 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.
- E. Plenum-Type, Paired, Readers and Wiegand Keypads Cable: Paired, 3 pairs, No. 22 AWG, stranded (7x30) tinned copper conductors, plastic insulation, individual aluminum foil-polypropylene tape shielded pairs each with No. 22 AWG, stranded tinned copper drain wire, 100 percent shield coverage, and fluorinated-ethylene-propylene jacket.
  - 1. NFPA 70, Type CMP.
  - 2. Flame Resistance: NFPA 262 Flame Test.
- F. Plenum-Type, Multiconductor, Readers and Wiegand 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.
- G. 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.
- H. Plenum-Type, Paired Input Cable: 1 pair, twisted, No. 22 AWG, stranded (7x30) tinned copper conductors, fluorinated-ethylene-propylene insulation, aluminum foil-polyester tape shield (foil side out), with No. 22 AWG drain wire, 100 percent shield coverage, and plastic jacket.
  - 1. NFPA 70, Type CMP.
  - 2. Flame Resistance: NFPA 262 Flame Test.

- I. Plenum-Type, Paired AC Transformer Cable: 1 pair, twisted, No. 18 AWG, stranded (19x30) tinned copper conductors, fluorinated-ethylene-propylene insulation, unshielded, and plastic jacket.
  - 1. NFPA 70, Type CMP.
  - 2. Flame Resistance: NFPA 262 Flame Test.

## **2.9 TRANSFORMERS**

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

## **PART 3 - EXECUTION**

### **3.1 EXAMINATION**

- A. Examine pathway elements intended for cables. Check for 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 systems to Controllers, card readers, and other cable-connected devices to determine the best retrofit method of providing cables into an existing door frame environment. Verify the actual "behind the wall and frame" structural elements before cutting or attempting to fish cables into the existing wall or frame. Surface mount raceway is acceptable, but only on concealed sides of the walls.
- C. Proceed with installation only after actual conditions have been researched.

### **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.
- 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. Wiring Method: Install wiring in raceway and cable tray, where possible. However, loose wiring may be installed within cabinets or in accessible ceiling spaces or in gypsum board partitions where unenclosed wiring method may be used. Use NRTL-listed plenum cable in air locations. Conceal raceway and cables except in unfinished spaces.
- C. 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.  
Install cables without damaging conductors, shield, or jacket.

### **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. Card Readers:
  - 1. Install number of conductor pairs recommended by manufacturer for the functions specified.
  - 2. For greater distances, install "extender" or "repeater" modules recommended by manufacturer of the Controller.
  - 3. Install minimum No. 18 AWG shielded cable to readers that draw 50 mA or more.
- D. Install minimum No. 16 AWG cable from Controller to electrically powered locks.

### **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. Install card reader and all associated monitoring devices at doors indicated.

### **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. 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. 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. Network Cable Procedures: Inspect for physical damage and test each conductor signal path for continuity and shorts. Use Class 2, bidirectional, Category 6 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.
  - 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.

- - - E N D - - -