SECTION 28 15 00

ACCESS CONTROL HARDWARE DEVICES

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. Card readers, credential cards, and keypads
2. Biometric identity-verification equipment
3. Cables
4. Transformers

1.3 DEFINITIONS

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

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

C. 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.

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

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

F. RAS: Remote access services.

G. RF: Radio frequency.

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

I. TCP/IP: Transport control protocol/Internet protocol.

J. 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.

K. WMP: Windows media player.

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

M. Open Supervised Device Protocol (OSDP): is a standard that has been developed by the Security Industry Association (SIA) in order to offer more secure access control communications. This protocol works across various types of readers, controllers, and software, and has been developed as a way to improve on issues of security that are often faced with other legacy systems.

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

1.4 ACTION SUBMITTALS

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

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

1. Diagrams for cable management system.
2. System labeling schedules, including electronic copy of labeling schedules that are part of the cable and asset identification system of the software specified in Parts 2 and 3.
3. Wiring Diagrams. For power, signal, and control wiring. Show typical wiring schematics including the following:
    a. Workstation outlets, jacks, and jack assemblies.
    b. Patch cords.
    c. Patch panels.
4. Cable Administration Drawings: As specified in "Identification" Article.
5. Battery and charger calculations for central station, workstations, and controllers.

C. Product Schedules.

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

1.5 INFORMATIONAL SUBMITTALS

A. Field quality-control reports.

1.6 CLOSEOUT SUBMITTALS

A. Operation and Maintenance Data: For security system to include in emergency, operation, and maintenance manuals. In addition to items specified in Section 017823 "Operation and Maintenance Data," include the following:

1. Hard copies of manufacturer's specification sheets, operating specifications, design guides, user's guides for software and hardware, and PDF files on cloud media of the hard-copy submittal.
2. System installation and setup guides with data forms to plan and record options and setup decisions.

1.7 MAINTENANCE MATERIAL SUBMITTALS

A. Furnish extra materials that match products installed and that are packaged with protective covering for storage and identified with labels describing contents.
  1. Credential card blanks, ready for printing. Include enough credential cards for all personnel to be enrolled at the site plus an extra 20 percent for future use.
  2. Fuses of all kinds, power and electronic, equal to 10 percent of amount installed for each size used, but no fewer than three units.

1.8 QUALITY ASSURANCE

A. Installer Qualifications: An employer of workers trained and approved by manufacturer.
  1. Cable installer must have on staff an RCDD certified by Building Industry Consulting Service International.

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

1.9 DELIVERY, STORAGE, AND HANDLING

A. 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.

B. 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.

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

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

PART 2 - PRODUCTS

2.1 ACCEPTABLE PRODUCTIONS ARE IDENTIFIED ON THE DRAWINGS.

2.2 OPERATION

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

2.3 PERFORMANCE REQUIREMENTS

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

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

2.4 CARD READERS, CREDENTIAL CARDS, AND KEYPADS

A. Part numbers are identified on the drawings.

B. Card-Reader Power: Powered from its associated controller, including its standby power source, and shall not dissipate more than 5 W.

C. 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.

D. Enclosure: Suitable for surface, semi-flush, pedestal, or weatherproof mounting. Mounting types shall additionally be suitable for installation in the following locations:

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

E. Touch-Plate and Proximity Readers:

1. The card reader shall read proximity cards in a range from direct contact to at least 6 inches (150 mm) from the reader.

F. Keypads:

1. Keypads shall contain an integral alphanumeric/special symbols keyboard with symbols arranged in ascending ASCII-code ordinal sequence.
2. Communication protocol shall be compatible with the local processor.

G. Keypad Response Time:

1. The keypad shall respond to passage requests by generating a signal to the local processor. The response time shall be 800 ms or less from the time the last alphanumeric symbol is entered until a response signal is generated.

H. Keypad Power:

1. The keypad shall be powered from the source as shown and shall not dissipate more than 150 W.

I. Keypad Mounting Method:

1. Keypads shall be suitable for surface, semi-flush, pedestal, or weatherproof mounting as required.

J. Communication Protocol: OSDP

K. Touch-Plate and Contactless Card Reader: The reader shall have "flash" download capability to accommodate card format changes. The card reader shall have capability of transmitting data to security control panel and shall comply with ISO/IEC 7816.

L. Credential Card Modification: Entry-control cards shall be able to be modified by lamination direct print process during the enrollment process without reduction of readability. The design of the credential cards shall allow for the addition of at least one slot or hole to accommodate the attachment of a clip for affixing the credential card to the badge holder used at the site.

2.5 BIOMETRIC IDENTITY-VERIFICATION EQUIPMENT

A. Biometric identity-verification templates shall be stored as part of system database files and used as a comparative base by the identity-verification equipment to generate an appropriate signal to the associated controller.

B. Fingerprint Analysis Scanner: Use a unique human fingerprint pattern to identify authorized, enrolled personnel. The design of this device shall incorporate positive measures to establish that the hand or fingers being scanned by the device belong to a living human being.

1. The user's hand shall remain in full view of the user at all times. The scan process of the fingerprint analysis scanner shall perform an optical or other type of scan of the enrollee's fingers. Scanning shall start automatically when the user's fingers are properly positioned.
2. Storage space for each fingerprint template shall not exceed 1250 8-bit bytes.
3. Template Update and Acceptance Tolerances: Fingerprint analysis scanners shall not automatically update an enrollee's profile. Significant changes in an individual's fingerprints shall require re-enrollment. Fingerprint analysis scanners shall provide an adjustable acceptance tolerance or template match criteria under system manager/operator control. Fingerprint analysis scanner shall determine when multiple attempts are needed for fingerprint verification and shall automatically prompt the user for additional attempts up to a maximum of three. Three failed attempts shall generate an entry-control alarm.
4. Average Verification Time: Fingerprint analysis scanner shall respond to passage requests by generating an entry request signal to the controller. The verification time shall be two seconds or less from the moment fingerprint analysis scanner initiates the scan process until fingerprint analysis scanner generates a response signal.
5. Modes: Fingerprint analysis scanner shall provide an enrollment mode, a recognition mode, and a code/credential verification mode.
   a. In the enrollment mode, fingerprint analysis scanner shall create a fingerprint template for new personnel and enter the template into the system database file created for that person.
   b. In the recognition mode, fingerprint analysis scanner shall allow passage when the fingerprint data from the verification attempt match a fingerprint template stored in database files.
   c. In the code/credential verification mode, fingerprint analysis scanner shall allow passage when the fingerprint data from the verification attempt match the fingerprint template associated with the identification code entered into a keypad, or they match the fingerprint template associated with credential card data read by a card reader.

6. Reports: Fingerprint analysis device shall create and store pattern match scores for all transactions involving fingerprint scans. Template match scores shall be stored in the matching personnel data file used for report generation.
7. Power: Fingerprint analysis scanner shall be powered from its associated controller, requiring not more than 45 W.
8. Enclosure: Scanners shall be available with enclosures that are suitable for surface, semiflush, or pedestal mounting. Mounting types shall additionally be suitable for installation in the following locations:
    a. Indoors, controlled environment.
    b. Indoors, uncontrolled environment.
9. Display: Digital visual indicator shall provide visible and audible status indications and user prompts. Indicate power on or off and whether user passage requests have been accepted or rejected.
10. Communication protocol: OSDP

2.6 CABLES

A. Acceptable part numbers shown on drawings.

2.7 TRANSFORMERS

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

PART 3 - EXECUTION

3.1 EXAMINATION

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

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

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

3.2 PREPARATION

A. Comply with recommendations in SIA CP-01.

B. Comply with TIA 606-B, "Administration Standard for Commercial Telecommunications Infrastructure."

C. Product Schedules: Obtain detailed product schedules from manufacturer of access-control system or develop product schedules to suit Project. Fill in all data available from Project plans and specifications and publish as Product Schedules for review and approval.

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

3.3 CABLING

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

B. Wiring Method: Install wiring in raceway and cable tray except within consoles, cabinets, desks, and counters. Conceal raceway and wiring except in unfinished spaces.

C. Wiring Method: Install wiring in raceway and cable tray except within consoles, cabinets, desks, and counters and except in accessible ceiling spaces and in gypsum board partitions where unenclosed wiring method may be used. Use NRTL-listed plenum cable in environmental airspaces, including plenum ceilings. Conceal raceway and cables except in unfinished spaces.

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

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

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

3.4 CABLE APPLICATION

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

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

C. TIA 232-F Cabling: Install at a maximum distance of 50 ft. (15 m) between terminations.

D. TIA 485-A Cabling: Install at a maximum distance of 4000 ft. (1220 m) between terminations.

E. Card Readers and Keypads:

1. Install number of conductor pairs recommended by manufacturer for the functions specified.
2. Unless manufacturer recommends larger conductors, install No. 22 AWG wire if maximum distance from controller to the reader is 250 ft. (75 m), and install No. 20 AWG wire if maximum distance is 500 ft. (150 m).

3. For greater distances, install "extender" or "repeater" modules recommended by manufacturer of the controller.
4. Install minimum No. 18 AWG shielded cable to readers and keypads that draw 50 mA or more.

F. Install minimum No. 16 AWG cable from controller to electrically powered locks. Do not exceed 500 ft. (150 m) between terminations.

G. Install minimum No. 18 AWG ac power wire from transformer to controller, with a maximum distance of 25 ft. (8 m) between terminations.

H. Open supervised device protocol (OSDP) must be used for all applicable security devices. Wiegand is not acceptable for devices that support OSDP.

3.5 GROUNDING

A. Comply with Section 270526 "Grounding and Bonding for Communications Systems."

B. Comply with IEEE 1100, "Recommended Practice for Power and Grounding Electronic Equipment."

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

D. Bond shields and drain conductors to ground at only one point in each circuit.

E. Signal Ground:
1. Terminal: Locate in each equipment room and wiring closet; isolate from power system and equipment grounding.
2. Bus: Mount on wall of main equipment room with standoff insulators.
3. Backbone Cable: Extend from signal ground bus to signal ground terminal in each equipment room and wiring closet.

3.6 INSTALLATION

A. Install card readers, keypads, push buttons, and biometric readers and local alarms.

3.7 IDENTIFICATION

A. In addition to requirements in this article, comply with applicable requirements in Section 270553 "Identification for Communications Systems" and with TIA 606-B.

B. Using software specified in "Cable and Asset Management Software" Article, develop cable administration drawings for system identification, testing, and management. Use unique, alphanumeric designation for each cable, and label cable and jacks, connectors, and terminals to which it connects with the same designation. Use logical and systematic designations for facility's architectural arrangement.

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

1. All wiring conductors connected to terminal strips shall be individually numbered, and each cable or wiring group being extended from a panel or cabinet to a building-mounted device shall be identified with the name and number of the particular device as shown.
2. Each wire connected to building-mounted devices is not required to be numbered at the device if the color of the wire is consistent with the associated wire connected and numbered within the panel or cabinet.

D. At completion, cable and asset management software shall reflect as-built conditions.

3.8 SYSTEM SOFTWARE AND HARDWARE

A. Develop, install, and test software and hardware, and perform database tests for the complete and proper operation of systems involved. Assign software license to Owner.

3.9 FIELD QUALITY CONTROL

A. Perform tests and inspections.

1. Manufacturer's Field Service: Engage a factory-authorized service representative to inspect components, assemblies, and equipment installations, including connections, and to assist in testing.

B. Tests and Inspections:

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

C. Devices and circuits will be considered defective if they do not pass tests and inspections.

D. Prepare test and inspection reports.

3.10 STARTUP SERVICE

A. Engage a factory-authorized service representative to supervise and assist with startup service.

1. Complete installation and startup checks according to approved procedures that were developed in "Preparation" Article and with manufacturer's written instructions.
2. Enroll and prepare badges and access cards for Owner's operators, management, and security personnel.

3.11 DEMONSTRATION

A. Engage a factory-authorized service representative to train Owner's maintenance personnel to adjust, operate, and maintain security access system. See Section 017900 "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 15 00