SECTION 281300 - 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 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. Samples: For workstation outlets, jacks, jack assemblies, and faceplates. For each exposed product and for each color and texture specified.

D. Other Action Submittals:

1. Project planning documents as specified in Part 3.

1.3 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. Microsoft Windows software documentation.

2. PC installation and operating documentation, manuals, and software for the PC and all installed peripherals. Software shall include system restore, emergency boot diskettes, and drivers for all installed hardware. Provide separately for each PC.
3. Hard copies of manufacturer's specification sheets, operating specifications, design guides, user's guides for software and hardware, and PDF files on CD-ROM of the hard-copy submittal.
4. System installation and setup guides with data forms to plan and record options and setup decisions.

1.4 MAINTENANCE MATERIAL SUBMITTALS

A. 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. Include 350.
2. Licenses. Provide licenses for each new piece of equipment.

1.5 QUALITY ASSURANCE

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

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

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

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

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

1.6 DELIVERY, STORAGE, AND HANDLING

A. A. Central Station, Workstations, and Controllers:

1. Store in temperature- and humidity-controlled environment in original manufacturer's sealed containers. Maintain ambient temperature between 50 and 85 deg F (10 and 30 deg C), and not more than 80 percent relative humidity, noncondensing.
2. Open each container; verify contents against packing list; and file copy of packing list, complete with container identification, for inclusion in operation and maintenance data.
3. Mark packing list with the same designations assigned to materials and equipment for recording in the system labeling schedules that are generated by software specified in "Cable and Asset Management Software" Article.
4. Save original manufacturer's containers and packing materials and deliver as directed under provisions covering extra materials.

1.7 PROJECT CONDITIONS

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

1. Indoor, Controlled Environment
2. Indoor, Uncontrolled Environment
3. Outdoor Environment
4. Hazardous Environment
5. Corrosive Environment

PART 2 - PRODUCTS

2.1 MANUFACTURERS

A. Basis-of-Design Product: Subject to compliance with requirements, provide Galaxy Control Systems.

2.2 DESCRIPTION

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

B. System Software: Based on existing Galaxy Control Systems architecture.

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

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

2.3 OPERATION

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

B. Distributed Processing: A fully distributed processing system.

C. System Network Requirements:

1. System components shall be interconnected and shall provide automatic communication of status changes, commands, field-initiated interrupts, and other communications required for proper system operation.
2. Communication shall not require operator initiation or response and shall return to normal after partial- or total-network interruption such as power loss or transient upset.
3. System shall automatically annunciate communication failures to the operator and shall identify the communications link that has experienced a partial or total failure.

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

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

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

1. Controllers shall serve as an interface between the central station and sensors and controls.
2. Data exchange between the central station and the controllers shall include down-line transmission of commands, software, and databases to controllers.
3. The up-line data exchange from the controller to the central station shall include status data such as intrusion alarms, status reports, and entry-control records.
4. Controllers are classified as alarm-annunciation or entry-control type.

2.4 FIXED MAP DISPLAY

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

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 90 minutes, complying with UL 924.

D. Entry-Control Controller:

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

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

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

1) On authentication of the credentials or information presented, check privileges of the identified individual, allowing only those actions granted as privileges.
2) Privileges shall include, but are not limited to, time of day control, day of week control, group control, and visitor escort control.

c. Maintain a date-, time-, and Location-stamped record of each transaction. A transaction is defined as any successful or unsuccessful attempt to gain access through a controlled portal by the presentation of credentials or other identifying information.

2. Inputs:

a. Data from entry-control devices; use this input to change modes between access and secure.
b. Database downloads and updates from the central station that include enrollment and privilege information.

3. Outputs:

a. Indicate success or failure of attempts to use entry-control devices and make comparisons of presented information with stored identification information.
b. Grant or deny entry by sending control signals to portal-control devices.
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 time listed in a schedule, alarm sounds.

4. With power supplies sufficient to power at voltage and frequency required for field devices and portal-control devices.

5. Controller Power: NFPA 70, Class II power-supply transformer, with 12- or 24-V ac secondary, backup battery and charger.

a. Backup Battery: Valve-regulated, recombinant-sealed, lead-calcium battery; spill proof; with a full one-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 Battery: Valve-regulated, recombinant-sealed, lead-acid battery; spill proof. With single-stage, constant-voltage-current, limited battery charger, comply with battery manufacturer's written instructions for battery terminal voltage and charging current recommendations for maximum battery life.
c. Backup Power-Supply Capacity: 90 minutes of battery supply. Submit battery and charger calculations.
d. Power Monitoring: Provide manual, dynamic battery-load test, initiated and monitored at the control center; with automatic disconnection of the controller

when battery voltage drops below controller limits. Report by using local controller-mounted digital displays and by communicating status to central station. Indicate normal power on and battery charger on trickle charge. Indicate and report the following:

1) Trouble Alarm: Normal power-off load assumed by battery.
2) Trouble Alarm: Low battery.
3) Alarm: Power off.

2.6 CARD READERS, CREDENTIAL CARDS, AND KEYPADS

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

B. Response Time: Card reader shall respond to passage requests by generating a signal that is sent to the controller. Response time shall be 800 ms or less, from the time the card reader finishes reading the credential card until a response signal is generated.

C. Communication Protocol: Compatible with local processor.

D. Credential: Match Existing.

2.7 CABLES

A. A. General Cable Requirements: Comply with requirements in Section 280513 "Conductors and Cables for Electronic Safety and Security" and as recommended by system manufacturer for integration requirement.

B. PVC-Jacketed, TIA 485-A Cables: Two pairs, twisted, No. 22 AWG, stranded (7x30) tinned copper conductors, PVC insulation, unshielded, PVC jacket, and NFPA 70, Type CMG.

C. Plenum-Type, TIA 485-A Cables:

1. Two pairs, No. 22 AWG, stranded (7x30) tinned copper conductors, fluorinated-ethylene-propylene insulation, unshielded, and fluorinated-ethylene-propylene jacket.
2. NFPA 70, Type CMP.
3. Flame Resistance: NFPA 262 flame test.

D. LAN Cabling:

1. Comply with requirements in Section 280513 "Conductors and Cables for Electronic Safety and Security."
2. NFPA 262.

2.8 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. In meetings with Architect and Owner, present Project planning documents and review, adjust, and prepare final setup documents. Use final documents to set up system software.

3.3 CABLING

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

B. Install cables and wiring according to requirements in Section 280513 "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 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 5E rating of components and fiber-optic rating of components, and that ensure Category 6 and fiber-optic performance of completed and linked signal paths, end to end.

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-B, "Commercial Building Standard for Telecommunications Pathways and Spaces."

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

C. TIA 485-A Cabling: Install at a maximum distance of 4000 ft..

D. 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., and install No. 20 AWG wire if maximum distance is 500 ft..
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.

E. Install minimum No. 16 AWG cable from controller to electrically powered locks. Do not exceed 500 ft..

3.5 GROUNDING

A. Comply with Section 260526 "Grounding and Bonding for Electrical Systems."

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

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

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

E. Signal Ground:

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

3.6 FIELD QUALITY CONTROL

A. Perform tests and inspections.

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

B. Tests and Inspections:

1. LAN Cable Procedures: Inspect for physical damage and test each conductor signal path for continuity and shorts. Use Class 2, bidirectional, Category 5 tester. Test for faulty connectors, splices, and terminations. Test according to TIA/EIA 568-B.1, "Commercial Building Telecommunications Cabling Standards - Part 1: General Requirements." Link performance for UTP cables must comply with minimum criteria in TIA/EIA 568-B.1.
2. Test each circuit and component of each system. Tests shall include, but are not limited to, measurements of power-supply output under maximum load, signal loop resistance, and leakage to ground where applicable. System components with battery backup shall be operated on battery power for a period of not less than 10 percent of the calculated battery operating time. Provide special equipment and software if testing requires special or dedicated equipment.
3. Operational Test: After installation of cables and connectors, demonstrate product capability and compliance with requirements. Test each signal path for end-to-end performance from each end of all pairs installed. Remove temporary connections when tests have been satisfactorily completed.
4. See Section 014000 "Quality Requirements" for retesting and reinspecting requirements and Section 017300 "Execution" for requirements for correcting the Work.

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

D. Prepare test and inspection reports.

3.7 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.

3.8 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.

3.9 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 281300