SECTION 283100

INTRUSION DETECTION

PART 1 - GENERAL

1.1 DESCRIPTION:

A. This Section covers intrusion detection systems.

1.2 RELATED SECTIONS:

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

B. Additional related specification sections include:

1. Section 280500, Common Work Results for Electronic Security.
2. Section 280513, Conductors and Cables for Electronic Security.
3. Section 280528, Pathways for Electronic Security.
4. Section 280800, Commissioning of Electronic Security.
5. Section 281000, Access Control.

1.3 QUALITY ASSURANCE:

A. Installation of the intrusion detection system shall be under the direct supervision of a person or persons having completed the factory training recommended by the system manufacturer.

B. The installation company shall be a currently listed as an authorized dealer or business partner by the manufacturer of the system and shall have been listed as such for a minimum of 3 years.

1.4 SUBMITTALS

A. See Section 280500, Common Work Results for Electronic Security for additional requirements.

B. Action Submittals:

1. Product Data:

a) Provide product data sheets for equipment, materials, and cables in PDF format.

2. Shop Drawings:

a) Include floor plans indicating equipment locations. Plans shall include equipment identification and either direct references to wiring details for each specific installation and wiring condition or a schedule that references the same.
b) Wiring diagrams shall indicate proposed connections of equipment, model numbers, and designations for cables and termination points.
c) Provide elevations of console or rack-mounted equipment, showing the location of all specified electronics and include enlarged, to scale plan (top), and front views.
d) Provide project specific manufacturer shop drawings of fabricated or modified

units, if any.

e) Provide riser diagrams indicating components of the system and proposed cabling between these components.
f) Provide block diagrams indicating the proposed interface between the intrusion detection system and the access control system. Provide a written description of the proposed sequence of operation to describe the operation of the interfaces.
g) Provide detailed project specific mounting diagram for each type of device including raceway and back box requirements. These details shall be referenced on the floor plans or schedules.
h) Provide a detailed loading schedule for each intrusion detection panel, identifying each device connected to it.

C. Informational Submittals: As required in Section 280500, Common Work Results for Electronic Security.

D. Close-out Submittals:

1. Functional Test Reports: Provide a spreadsheet with all intrusion detection system devices and major components listed in the first column by device designator (e.g., device number) with each test parameter listed by name (or code) in the remaining columns.
2. Operations and Maintenance Documentation Package: As defined in Section 280500, Common Work Results for Electronic Security.
3. Instruction of Operating Personnel:

a) The Security Systems Performance Verification Supervisor shall schedule, coordinate, assemble and deliver the documentation of the training required by this section.
b) Obtain receipt from the Owner acknowledging completion of each item of instruction.
c) See Section 280500, Common Work Results for Electronic Security for additional requirements.

PART 2 - PRODUCTS

2.1 DETECTION DEVICES:

A. Magnetic Contacts:

1. For hinged doors: 0.75" round recessed switches for door head installation. Switches shall be magnetic, double-pole, double-throw type, providing dual circuit operation, designed for line supervision. Switches shall be tested and proven capable of initiating an alarm signal when the protected door is opened 2" on the latch side. Color of exposed portions of the door contacts (brown, grey, or white) shall be that which most closely matches the door frame color.
2. For overhead doors: extra heavy duty, aluminum bar stock construction, floor-mounted contact, double-pole, double-throw type, providing dual circuit operation, for use on roll-up doors and rolling gates. Contacts shall have 3' stainless steel armored cables.
3. Alarm contacts shall be designed for 12 V to 30 V DC, nonpolarized service.
4. Manufacturer: GRI, Nascom or Sentrol.

B. Duress Devices:

1. Push-for-Help Buttons:

a) Designed for mounting under counter.
b) Latching call-placed indicator.
c) Manufacturer: Ademco, or Sentrol.

C. Glass Break Detectors:

1. Sensors shall use microprocessor-based digital signal processing to convert sound into mathematical sequences and perform analysis on signal variables to accurately identify the signal pattern of breaking glass.
2. Signal variables shall include flex/audio thresholds, ratios and durations, time coincidence, attack thresholds, and microphone overloads.
3. Detectors shall be configured with 2 microphones, 180º opposed, and time-of-arrival processing to eliminate glass break signals arriving from other than the protected area.
4. Detectors shall also provide the following minimum features:

a) Form C (SPDT) alarm relay rated for 25 V DC, 125 mA maximum.
b) Combination cover and wall tamper switch rated for 24 V DC, 25 mA maximum.
c) LED indication for detection of sound events and alarm condition.
d) Minimum range: 25'.
e) Radio frequency interference (RFI) immunity from 10 MHz to 1000 MHz, up to 30 Vm.
f) Capable of detecting the breaking of single-pane plate, laminated, tempered, wired, and film-coated glass up to 0.25" thick.
g) Supervision circuitry with trouble output rated for 16 V DC, 20 mA maximum.

5. Manufacturer: Honeywell FG-1625 RT or approved equal.

D. Interior Motion Detectors:

1. Dual technology microwave and infrared motion type with the following minimum features:

a) Walk-test light.
b) X-Band (10.525 GHz) microwave technology with automatic range adjustment on microwave sensor to account for repetitive moving objects which are not intrusion attempts.
c) Anti-masking.
d) Selectable look-down zone.
e) Tamper alarm switch.
f) Digital fluorescent light interference filter.
g) RFI immunity: 27 MHz to 825 MHz.
h) White light immunity up to 650 fc.
i) Dual slope temperature compensation.
j) Form C output relay rated for 3 W.
k) Self-test: microwave supervision, end-to-end PIR, and temperature compensation.
l) Integrated end-of-line resistor.
m) FCC certified and UL listed.

n) Service: 10.5 V DC to 14 V DC.
o) Coverage Pattern:

1) Wall mount: minimum 50' x 70'.
2) Ceiling mount: vertical range 8’ to 25’, horizontal coverage pattern 360° minimum 60' diameter.

2. Manufacturer: Bosch, Honeywell or approved equal.

2.2 INTRUSION DETECTION SYSTEMS (IDS):

A. General:

1. Provide a microprocessor-based control/digital communicator that can provide intrusion, duress, and critical equipment monitoring. The system shall have a minimum of 48 individually addressable points that can transmit signals to a central station receiver. The system shall have the capability of controlling up to 16 outputs.
2. The system shall have arming stations with a touch pad through which users control security functions. Arming stations shall also have a minimum 16-character alphanumeric display. Displays shall show system status and give prompts to system operation. Arming stations shall display the status of 48 separate protection zones.
3. The system shall accommodate up to 8 microprocessor-based arming stations. All system operations shall be accomplished at any arming station.

B. Initiation Circuits:

1. Protective inputs shall consist of points designated burglary and/or hold-up-duress and/or fire and/or supervisory. Each point shall be monitored by a protective circuit and shall accommodate normally opened and normally closed devices with end-of-line resistor supervision, or encrypted communication supervision.
2. Point programming: each of the points shall be programmable as to whether they are controlled versus 24 hours, interior versus perimeter, instant versus delayed, silent versus audible, and local or reporting. Additionally, each point shall be programmable to report to three separate telephone numbers.

C. Output Circuits:

1. Alarm power outputs: shall power audible alarms. Alarm circuits shall be supervised. There shall be 4 distinct audible patterns from which to select.
2. Additional relay outputs: capacity to connect to the ACAMS for zone level system integration.

D. System Partitioning:

1. Point assignment: points shall be assignable to 1 of a minimum of 4 areas of protection.
2. Area arming: each area shall be separately armed and disarmed from any of the arming stations. Area 1 shall have the option of being a shared area that disarms automatically with the first area disarmed and arms automatically when the second area is armed. Alternately, area 1 can be a master area that cannot be armed until areas 2, 3, and 4 are armed.]
3. Keyswitch arming inputs: shall be programmable as either maintained or momentary contact.

E. Miscellaneous:

1. Programming: system functions shall be programmable at the system site or remotely via the use of the dial-up telephone network. Minimum programmable system passcode shall be used to prevent unauthorized remote programming attempts. Telephone access to the system shall be a ring counter or user-initiated access.
2. Remote keypads: shall allow arming and disarming of the system, shunting of individual zones, and adjusting any delay periods.

F. Manufacturer: Bosch, Digital Monitoring Products (DMP), Digital Security Controls (DSC), or approved equal.

PART 3 - EXECUTION

3.1 GENERAL:

A. Programming:

1. Program alarm response fields, door names, and any other user-defined fields with terminology and descriptions provided by the Owner.
2. Program access rights, password protection, holidays, area control, inputs and outputs, and schedules.

B. Graphics:

1. Develop graphic maps that detail the facility and display inputs and outputs dynamically.
2. Utilize AutoCAD architectural floor plans that show walls, doors, windows, room names, and room numbers.

C. System Integration and Interfaces:

1. Interface with the access control system via hardware interface. Provide an output for each zone of detection that shall be connected to an input on the ACAMS.
2. Coordinate zoning requirements with the Owner.

D. Programming Requirements and Deliverables:

1. Produce questionnaires to solicit user input for programming the system. The questionnaires shall identify each programming item that requires user input to configure the ACAMS along with recommendations for responses. These questionnaires shall be finalized in a series of meetings with the Owner's designated agent until such time that the questionnaires are completed, and the Owner has authorized the information to be entered into the ACAMS.
2. The questionnaires shall include three series. The first shall be devoted to alarm input related programming. The second shall be devoted to interface programming and associated action and reaction requirements including the video surveillance system call-up and switching requirements. The third shall be related to display of alarm messaging, mapping and any requirements for alarm responses and reporting.
3. Upon completion, the programming questionnaires and associated programming database sheets shall be included in the operation and maintenance documentation.

E. Each alarm event shall result in the following actions:

1. A supervised and coded alarm signal shall be transmitted to the associated workstations or consoles causing an audible and visual alarm signal.
2. A graphical representation of the alarm scene (site or floor plan) with icons

representing the open door, video camera, and other local devices shall be displayed on the graphical user interface (GUI). Icons representing active devices shall change color to indicate their state change (inactive to active).

3.2 FIELD QUALITY CONTROL

A. Tests and Inspections:

1. One at a time breach each device in each zone that makes up the intrusion detection system. Where the intrusion detection system is designed to detect multiple types of breaches, test each zone or device using each type of breach that is practical without damaging the system or system components. Provide a glass break simulator for testing glass break detectors. For each intrusion point, test the following parameters or functions:

    a) Event is logged and displayed on the keypad and the security workstation with operator instructions.
    b) Where a local door sounder is located adjacent to the door, the event activates the sounder alarm until reset at the workstation or console.
    c) On the GUI, the event causes icons representing active devices to change color to indicate their state change (inactive to active).

B. Test Reports:

1. Print a report showing the alarm activity for the test period. Confirm that the report shows an alarm or exception appropriate for the zone and breach for each intrusion detection or duress alarm zone or device in the system. Present this report to the Owner.

3.3 INSTRUCTION OF OPERATING PERSONNEL

A. Factory-trained technicians shall give operating and maintenance instructions on the intrusion detection system equipment. The duration of each session for each system type shall be a minimum of 8 hours.

B. See Section 280500, Common Work Results for Electronic Security for additional requirements.

END OF SECTION 283100