SECTION 281600 - INTRUSION DETECTION

Latest Update 5-7-2017 See underlined text for Edits.

(Engineer shall edit specifications and blue text in header to meet project requirements. This includes but is not limited to updating Equipment and/or Material Model Numbers indicated in the specifications and adding any additional specifications that may be required by the project. Also turn off all "Underlines".)

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 and all other sections of Division 28.

1.2 SUMMARY

A. Section Includes:

1. Intrusion detection with communication links to perform monitoring, alarm, and control functions.
2. Integration of other electronic and electrical systems and equipment.

1.3 DEFINITIONS

A. CCTV: Closed-circuit television.

B. PIR: Passive infrared.

C. RFI: Radio-frequency interference.

D. UPS: Uninterruptible power supply.

E. Control Unit: System component that monitors inputs and controls outputs through various circuits.

F. Master Control Unit: System component that accepts inputs from other control units and may also perform control-unit functions. The unit has limited capacity for the number of protected zones and is installed at an unattended location or at a location where it is not the attendant's primary function to monitor the security system.

G. Monitoring Station: Facility that receives signals and has personnel in attendance at all times to respond to signals. A central station is a monitoring station that is listed.

H. Protected Zone: A protected premises or an area within a protected premises that is provided with means to prevent an unwanted event.

I. Standard Intruder: A person who weighs one hundred (100) lbs or less and whose height is sixty (60) inches or less; dressed in a long-sleeved shirt, slacks, and shoes.

J. Standard-Intruder Movement: Any movement, such as walking, running, crawling, rolling, or jumping, of a "standard intruder" in a protected zone.

K. Systems Integration: The bringing together of components of several systems containing interacting components to achieve indicated functional operation of combined systems.

L. Zone: A zone is a defined area; within a protected premises. It is a space or area for which an intrusion must be detected and uniquely identified. The sensor or group of sensors must then be assigned to perform the detection, and any interface equipment between sensors and communication must link to master control unit.

1.4 ACTION SUBMITTALS

A. Product Data: Components for sensing, detecting, systems integration, and control, 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 including interconnections between components specified in this Section and those furnished under other Sections. Indicate methods used to achieve systems integration. Indicate control, signal, and data communication paths and identify networks control interface devices and media to be used. Describe characteristics of network and other data communication lines.

    a. Indicate methods used to achieve systems integration.
    b. Indicate control, signal, and data communication paths and identify PLCs, networks, control interface devices, and media to be used.
    c. Describe characteristics of network and other data communication lines.
    d. Describe methods used to protect against power outages and transient voltages including types and ratings of isolation and surge suppression devices used in data, communication, signal, control, and ac and dc power circuits.

2. Raceway Riser Diagrams: Detail raceway runs required for intrusion detection and for systems integration. Include designation of devices connected by raceway, raceway type and size, and type and size of wire and cable fill for each raceway run.

3. UPS: Sizing calculations.
4. Site and Floor Plans: Indicate final outlet and device locations, routing of raceways, and cables inside and outside the building.
5. Device Address List: Coordinate with final system programming.
6. System Wiring Diagrams: Include system diagrams unique to Project. Show connections for all devices, components, and auxiliary equipment. Include diagrams for equipment and for system with all terminals and interconnections identified.
7. Details of surge-protection devices and their installation.
8. Sensor detection patterns and adjustment ranges.

C. Equipment and System Operation Description: Include method of operation and supervision of each component and each type of circuit. Show sequence of operations for manually and automatically initiated system or equipment inputs. Description must cover this specific Project; manufacturer's standard descriptions for generic systems are unacceptable.

D. Samples for Initial Selection: For units with factory-applied color finishes.

1.5 INFORMATIONAL SUBMITTALS

A. Qualification Data: For Installer and intrusion detection systems integrator and testing agency.

B. Field quality-control reports.

C. Warranty: Sample of special warranty.

D. Other Information Submittals:

1. Test Plan and Schedule: Test plan defining all tests required to ensure that system meets technical, operational, and performance specifications within 60 days of date of Contract award.
2. Examination reports documenting inspections of substrates, areas, and conditions.
3. Anchor inspection reports documenting inspections of built-in and cast-in anchors.

1.6 CLOSEOUT SUBMITTALS

A. Operation and Maintenance Data: For intrusion detection 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. Data for each type of product, including features and operating sequences, both automatic and manual.

2. Master control-unit hardware and software data.

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. Intrusion Detection Devices: Furnish quantity equal to 5% of the number of units of each type installed, but no fewer than one of each type.
2. Fuses: Three (3) of each kind and size.
3. Security Fasteners: Furnish no fewer than one (1) box for every fifty (50) boxes or fraction thereof, of each type and size of security fastener installed.

1.8 QUALITY ASSURANCE

A. Installer Qualifications:

1. An employer of workers, at least one of whom is a technician certified by the National Burglar & Fire Alarm Association.
2. Manufacturer's authorized representative who is trained and approved for installation of units required for this Project.

B. Intrusion Detection Systems Integrator Qualifications: An experienced intrusion detection equipment supplier who has completed systems integration work for installations similar in material, design, and extent to that indicated for this Project, whose work has resulted in construction with a record of successful in-service performance.

C. Testing Agency Qualifications: Member company of NETA or an NRTL.

1. Testing Agency's Field Supervisor: Currently certified by NETA to supervise on-site testing.

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.

E. Control Units, Devices, and Communications with Monitoring Station: Listed and labeled by a qualified testing agency for compliance with SIA CP-01.

F. Comply with NFPA 70.

G. The alarm manufacturer shall be certified as being compliant with ISO9001.

H. State of the Art Development

1. Supply only the manufacturer's latest developed product. In cases where product development surpasses the criteria of the specification make the newer product available to the project at no additional cost. In no case shall discontinued or obsolete equipment be acceptable. The same requirement applies to software programs developed/updated during the warranty period.
2. Should the product recall by the manufacturer require temporary or permanent replacement of a product specified under this section, notify the Architect at the earliest reasonable time and arrange to replace the product in question at the earliest possible time.

    a. Equipment found defective or subject to recall prior to scheduled installation shall not be delivered to the jobsite.
    b. Equipment defect or intended recall shall not relieve the manufacturer from his contractual obligation with regard to delivery schedule of product.
    c. Under no circumstances shall arrangement for alternate product necessarily require the Owner to accept superseded equipment except on a temporary basis.

1.9 PROJECT CONDITIONS

A. Environmental Conditions: Capable of withstanding the following environmental conditions without mechanical or electrical damage or degradation of operating capability:

1. Master Control Unit: Rated for continuous operation in an ambient of 60^0F to 85^0F and a relative humidity of 20% to 80 % noncondensing.
2. Interior, Controlled Environment: System components, except master control unit, installed in temperature-controlled interior environments shall be rated for continuous operation in ambient of 36^0F to 122^0F dry bulb and 20% to 90% relative humidity, noncondensing.
3. Interior, Uncontrolled Environment: System components installed in non-temperature-controlled interior environments shall be rated for continuous operation in ambient of 0^0F to 122^0F dry bulb and 20% to 90% relative humidity, noncondensing.
4. Exterior Environment: System components installed in locations exposed to weather shall be rated for continuous operation in ambient of minus 30^0F to plus 122^0F dry bulb and 20% to 90% relative humidity, condensing. Comply with UL 294 and UL 639 for outdoor-use equipment. Rate for continuous operation when exposed to rain as specified in NEMA 250, winds up to eighty five (85) mph and snow cover up to twenty four (24) inches thick.
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 or flyings shall be rated, listed, and installed according to NFPA 70.

1.10 WARRANTY/GUARANTEE

A. See Division 26 Specification Section "Basic Electrical Requirements' for warranty and guarantee requirements.

B. Special Warranty: Manufacturer's standard form in which manufacturer and Installer agree to repair or replace components of intrusion detection devices and equipment that fail in materials or workmanship within specified warranty period.

PART 2 - PRODUCTS

2.1 FUNCTIONAL DESCRIPTION OF SYSTEM

A. Description: Multiplexed, modular, microprocessor-based controls, intrusion sensors and detection devices, and communication links to perform monitoring, alarm, and control functions.

B. Supervision: System components shall be continuously monitored for normal, alarm, supervisory, and trouble conditions. Indicate deviations from normal conditions at any location in system. Indication includes identification of device or circuit in which deviation has occurred and whether deviation is an alarm or malfunction.

1. Alarm Signal: Display at master control unit and actuate audible and visual alarm devices.
2. Trouble Condition Signal: Distinct from other signals, indicating that system is not fully functional. Trouble signal shall indicate system problems such as battery failure, open or shorted transmission line conductors, or control-unit failure.
3. Supervisory Condition Signal: Distinct from other signals, indicating an abnormal condition as specified for the particular device or control unit.

C. System Control: Master control unit shall directly monitor intrusion detection devices and connecting wiring in a multiplexed distributed control system or as part of a network.

D. System shall automatically reboot program without error or loss of status or alarm data after any system disturbance.

E. Operator Commands:

1. Help with System Operation: Display all commands available to operator. Help command, followed by a specific command, shall produce a short explanation of the purpose, use, and system reaction to that command.
2. Acknowledge Alarm: To indicate that alarm message has been observed by operator.
3. Place Protected Zone in Access: Disable all intrusion-alarm circuits of a specific protected zone. Tamper circuits may not be disabled by operator.

4. Place Protected Zone in Secure: Activate all intrusion-alarm circuits of a protected zone.
5. Protected Zone Test: Initiate operational test of a specific protected zone.
6. System Test: Initiate system-wide operational test.
7. Print reports.

F. Timed Control at Master Control Unit: Allow automatically timed "secure" and "access" functions of selected protected zones.

G. Automatic Control of Related Systems: Alarm or supervisory signals from certain intrusion detection devices control the following functions in related systems:

1. Switch selected lights.
2. Shift elevator control to a different mode.
3. Open a signal path between certain intercommunication stations.
4. Shift sound system to "listening mode" and open a signal path to certain system speakers.
5. Switch signal to selected monitor from CCTV camera in vicinity of sensor signaling an alarm.

H. Printed Record of Events: Print a record of alarm, supervisory, and trouble events on system printer. Sort and report by protected zone, device, and function. When master control unit receives a signal, print a report of alarm, supervisory, or trouble condition. Report type of signal (alarm, supervisory, or trouble), protected zone description, date, and time of occurrence. Differentiate alarm signals from other indications. When system is reset, report reset event with the same information concerning device, location, date, and time. Commands shall initiate the reporting of a list of current alarm, supervisory, and trouble conditions in system or a log of past events.

I. Response Time: Five seconds between actuation of any alarm and its indication at master control unit.

J. Circuit Supervision: Supervise all signal and data transmission lines, links with other systems, and sensors from master control unit. Indicate circuit and detection device faults with both protected zone and trouble signals, sound a distinctive audible tone, and illuminate an LED. Maximum permissible elapsed time between occurrence of a trouble condition and indication at master control unit is twenty (20) seconds. Initiate an alarm in response to opening, closing, shorting, or grounding of a signal or data transmission line.

K. Programmed Secure-Access Control: System shall be programmable to automatically change status of various combinations of protected zones between secure and access conditions at scheduled times. Status changes may be preset for repetitive, daily, and weekly; specially scheduled operations may be preset up to a year in advance. Manual secure-access control stations shall override programmed settings.

L. Manual Secure-Access Control: Coded entries at manual stations shall change status of associated protected zone between secure and access conditions.

M. Provide a completely functional intrusion detection system that includes the following capabilities:

1. Listed for UL Commercial Burglary
2. Supports up to two hundred fifty (250) zones.
3. Supports up to eight (8) separate partitions.
4. Supports up to two hundred fifty (250) users.
5. Provides integrated security, access control, and CCTV switching capability.
6. Provides supervision of peripheral devices.
7. Supports up to ninety six (96) optional relay outputs.
8. Supports long-range radio (LRR) communication.
9. Provides scheduling capability to allow for automated operations.
10. Supports up to eight (8) alphanumeric paging devices.
11. Supports panel linking.
12. Supports alarm reporting via Internet.
13. Interfaces with automation software.
14. Capable of being installed using existing wiring.

2.2 SYSTEM COMPONENT REQUIREMENTS

A. Control Panel: The Honeywell Vista 250BP control panel shall be an eight (8)-partition, UL commercial burglary control panel that supports up to two hundred fifty (250) zones using basic hardwired, polling loop, and wireless zones. It shall also provide supervision of the bell output, RF receivers, and relay modules. In addition, the control shall provide the ability to schedule time-driven events, and allow certain operations to be automated by pressing a single button. The system shall be capable of interfacing with an ECP long range radio (LRR) unit that can send Contact ID messages, and alphanumeric paging devices. The control shall provide integrated access control and CCTV-switching capability.

1. Basic Hardwired Zones: The control shall provide nine (9) style-B hardwire zones with the following characteristics:

   a. EOLR supervision (optional for zones 2-8): Shall support N.O. or N.C. sensors (EOLR supervision required for UL installations).
   b. Individually assignable to one of eight (8) partitions.
   c. Support up to sixteen (16) two (2) wire smoke detectors on one selected zone.
   d. Support four-wire smoke or heat detectors on any zone (power to four-wire smoke detectors must be supervised with an EOL device).
   e. Support up to fifty (50) two (2) wire latching glass break detectors on one selected zone.

2. Commercial Wireless Equipment: The Control shall be compatible with UL Listed Commercial Wireless Security equipment including but not limited to:

   a. ADEMCO 5817CB (5814, 5815, 5816, 5916MN, 5817 and 5818) Wireless Universal Contact Monitoring Transmitter - This device shall be capable of making any conventional UL listed contact device a wireless device. The device shall be UL listed as follows: UL 985 for fire and UL 365, 609, 1023, 1076 and 1610 for security.
   b. ADEMCO 5869 Wireless Hold Up Switch/Transmitter – This device shall be UL 636 listed for commercial burglary applications.
   c. ADEMCO 5897-35 Wireless Dual Tec Motion Sensors - This device shall be UL 636 listed for commercial burglary applications.
   d. ADEMCO 5853 Wireless Glass-break Detectors - This device shall be UL 636 listed for commercial burglary applications.
   e. ADEMCO 5800SS1 – Wireless Shock Sensors - This device shall be UL 636 listed for commercial burglary applications.
   f. ADEMCO 5808LST Wireless Heat/Smoke Sensor- This device is UL 268 listed for use in both commercial and residential applications.

3. Optional Expansion Zones

   a. Polling Loop Expansion: The control shall support up to two hundred forty one (241) additional hardwire zones using a built-in two-wire polling (multiplex) loop interface. The polling loop shall provide power and data to remote point modules, and constantly monitor the status of all zones on the loop. Maximum current draw shall not exceed 128 mA. The polling loop zones shall have the following characteristics:

      1) Interface with RPM (Remote Point Module) devices that provide Class B, Style Y (e.g., 4208U/4208SN) or a combination of Class B, Style Y, and Class A, Style Z (e.g., 4208SNF) zones.
      2) Individually assignable to one of eight (8) partitions.
      3) Supervised by the control panel.
      4) A 12,000 ft (3658 m) wire run capability without using shielded cable.
      5) Each RPM (Remote Point Module) enclosure shall be tamper protected.

   b. Wireless Expansion: The control shall support up to two hundred fifty (250) wireless zones using a 5800 series RF receiver (fewer if using hardwire and/or polling loop zones). Wireless zones shall have the following characteristics:

      1) Supervised by control panel for check-in signals (except certain non-supervised transmitters).
      2) Tamper-protection for supervised zones.

3) Individually assignable to one (1) of eight (8) partitions.
4) Support wireless devices listed for Commercial Burglary using the 5881ENHC RF Receiver.

4. Partitions: The control shall provide the ability to operate eight (8) separate areas, each functioning as if it had its own control. Partitioning features shall include:

a. A Common Lobby partition (1-8), which can be programmed to perform the following functions:

1) Arm automatically when the last partition that shares the common lobby is armed.
2) Disarm when the first partition that shares the common lobby is disarmed.

b. A Master partition (9), used strictly to assign keypads for the purpose of viewing the status of all eight (8) partitions at the same time (master keypads).
c. Assignable by zone.
d. Assignable by keypad.
e. Assignable by relay to one or all eight (8) partitions.
f. Ability to display fire and/or burglary and panic and/or trouble conditions at all other partitions' keypads (selectable option).
g. Certain system options selectable by partition, such as entry/exit delay and subscriber account number.

5. User Codes: The control shall accommodate two hundred fifty (250) user codes, all of which can operate any or all partitions. Certain characteristics must be assignable to each user code, as follows:

a. Authority level (Master, Manager, or several other Operator levels). Each User Code (other than the installer code) shall be capable of being assigned the same or a different level of authority for each partition that it will operate.
b. Opening/Closing central station reporting option.
c. Specific partitions that the code can operate.
d. Global arming capability (ability to arm all partitions the code has access to in one command).
e. Use of an RF (button) to arm and disarm the system (RF key must first be enrolled into the system).

6. Peripheral Devices: The control shall support up to thirty (30) addressable ECP devices, which can be any combination of keypads, RF receivers, relay modules, annunciator modules, and interactive phone modules. Peripheral devices have the following characteristics:

a. Each device set to an individual address according to the device's instructions.
b. Each device enabled in system programming.
c. Each device's address shall be supervisable (via a programming option).

7. 6. Keypad/Annunciator: The control shall accommodate up to sixteen (16) keypads or six (6) touch-screen (i.e.; advanced user interface) keypads. The keypads shall be capable of the following:

a. Performing all system arming functions.
b. Being assigned to any partition.
c. Providing four programmable single-button function keys, which can be used for:

1) Panic Functions: Activated by wired and wireless keypads; reported separately by partition.
2) Keypad Macros: Thirty two (32) keypad macro commands per system (each macro is a series of keypad commands). Assignable to the A, B, C, and D keys by partition.

8. Optional Output Relays: A total of ninety six (96) relay outputs shall be accommodated using relay modules. Each relay module shall provide four (4) Form C (normally open and normally closed) relays for general purpose use or two (2) Class-B, Style-Y supervised notification appliance circuit outputs, when using the 4204CF module. The relays shall be capable of being:

a. Programmed to activate in response to system events.
b. Programmed to activate using time intervals.
c. Activated manually.
d. Assigned an alpha descriptor.
e. Used for Class B, Style-Y supervised bell outputs (4204CF module).
f. A combination of 4204 (ECP) and 4101SN (polling loop) relays.

9. Optional Vista Interactive Phone Module: The control shall support the ADEMCO 4285/4286 VIP Modules, which permit access to the security system in order to perform the following functions:

a. Obtain system status information.
b. Arm and disarm the security system.
c. Control relays.

10. Optional LED Annunciator: The control shall support the ADEMCO FSA-8 and FSA-24 annunciators, which are capable of:

a. Visually identifying a zone or point that is in alarm or trouble.
b. Programmable for system silence/reset.

c. Up to 96 LEDs may be used in one system.
d. A total of four (4) FSA-24 or 12 FSA-8 annunciators may be used in one system.
e. An optional key-switch, FSAKSM module, shall be available for UL listed Silence and Reset capability.

11. Integrated Access Control: The control shall be capable of the following:

a. Providing a command that activates relays to allow access doors to open (e.g., lobby door), lights to be turned on or off, etc.
b. Becoming a fully integrated access control system by using numerous VistaKey Single-Door Access Control Modules.
c. Supporting up to fifteen (15) VistaKey Access Control Modules. The VistaKey Access Control Modules shall use the same Compass Downloader as the Vista-250BP and shall be programmable from the Compass Downloader or the Keypad/Annunciators.
d. Assigning any number of access control relays to each partition (up to ninety six (96) for the system).
e. Supporting up to five hundred (500) access card holders using VistaKey.
f. Connecting to the ADEMCO PassPoint Access Control System via the Vista Gateway Module (VGM).

12. CCTV Switching: The System shall be capable of supporting the VistaView 100 CCTV Switching System. The CCTV system shall be fully integrated and be event driven by Fire, Burglary or Access events. When cameras are not event driven, they shall be driven by an automatic preset dwell time. The system shall also be capable of:

a. Activating the CCTV system via a Form-C relay output.
b. Operating up to sixty (60) camera inputs and thirty (30) video outputs.

13. Optional Keyswitch: The control shall support the ADEMCO 4146 Keyswitch on any one of the system's eight (8) partitions. If used, zone 7 is no longer available as a protection zone.
14. Voltage Triggers: The system shall provide voltage triggers, which change state for different conditions. Used with LRR (Long Range Radio) equipment or other devices such as a remote keypad sounder, Keyswitch ARMED and READY LEDs, or a printer to print the system's event log.
15. Event Log: The System shall maintain a log of different event types (enabled in programming). The event log shall provide the following characteristics:
a. Stores up to one thousand (1,000) events.
b. Viewable at the keypad or through the use of Compass software.
c. Printable on a serial printer using a 4100SM Module including zone alpha descriptors.
d. Stores Pass Point access control events.
e. Sends printed events to up to eight (8) alphanumeric pagers.

16. Scheduling: Provides the following scheduling capabilities:
    a. Open/close schedules (for control of arming/disarming and reporting).
    b. Holiday schedules (allows different time windows for open/close schedules).
    c. Timed events (for activation of relays, auto-bypassing and unbypassing, auto-arming and disarming, etc.).
    d. Access schedules (for limiting system access to users by time)
    e. End User Output Programming Mode (provides twenty (20) timers for relay control).
    f. The system shall automatically adjust for daylight savings time.

17. Communication Features: Supports the following formats and features for the primary and secondary central station receivers:

    a. Formats

        1) ADEMCO Low Speed (Standard or Expanded).
        2) Sescoa/Radionics.
        3) ADEMCO Express.
        4) ADEMCO High Speed.
        5) ADEMCO Contact ID.

    b. Backup Reporting: The system shall support backup reporting via the following:

        1) Secondary phone number.
        2) ECP long-range radio (LRR) interface.
        3) Option to select long range radio (LRR) or dialup as the primary reporting method (dynamic signaling feature).

    c. Internet Reporting: The system shall be capable of communicating with the central station via the internet using Alarmnet:

        1) It shall provide the user with the ability to control the system via a browser interface (i.e., AOL, Netscape, and Internet Explorer). All packet data transmitted to the monitoring station shall be encrypted with a minimum of one thousand twenty four (1,024) bits of encryption.

18. Audio Alarm Verification Option: Provides a programmable Audio Alarm Verification (AAV) option that can be used in conjunction with an output relay to permit voice dialog between an operator at the central station and a person at the premises.
19. Cross-Zoning Capability: Helps prevent false alarms by preventing a zone from going into alarm unless its cross-zone is also faulted within five (5) minutes.

20. Pager Interface: The Control Panel shall be capable of sending event information to an alphanumeric pager via a VA-8201 pager interface device.
21. Exit Error False Alarm Prevention Feature: The System shall be capable of differentiating between an actual alarm and an alarm caused by leaving an entry/exit door open. If not subsequently disarmed, the control panel shall:

    a. Bypass the faulted E/E zone(s) and/or interior zones and arm the system.
    b. Generate an Exit Error report by user and by zone so the central station knows it was an exit alarm and who caused it.

22. Built-in User's Manual and Descriptor Review: For end-user convenience, the control panel shall contain a built-in User's Manual. It shall include the following capabilities:

    a. By depressing any of the function keys on the keypad for five (5) seconds, a brief explanation of that function shall scroll across the alphanumeric display.
    b. By depressing the READY key for five (5) seconds, all programmed zone descriptors shall be displayed (one at a time). This feature shall provide a check for installers and ensure all descriptors have been entered properly.

23. Programming: The Control shall be capable of being programmed locally or remotely using the ADEMCO Compass Downloader and shall be capable of:

    a. Uploading and downloading all programming information at 300 baud.
    b. Uploading and displaying firmware revision levels from the control.

24. Panel Linking: The Control shall be capable of being networked together with up to eight other controls and being operated by any keypad within the system. It shall provide the ability for users to:

    a. Control multiple zones, partitions, and/or buildings from a central location.
    b. Check status, arm and disarm any partition from any keypad in the system.
    c. Globally arm or disarm partitions based upon user authority.

25. Automation Software: The Control shall be capable of interfacing with automation software via an RS232 input on a single partition. The control panel shall be the ADEMCO VISTA-250BP Commercial Burglary Partitioned Security System or equivalent.

B. Compatibility: Detection devices and their communication features, connecting wiring, and master control unit shall be selected and configured with accessories for full compatibility with the following equipment:

    1. Door hardware specified in Section 087100 "Door Hardware."

2. Elevators specified in Section 142400 "Hydraulic Elevators."
3. Lighting controls specified in Section 260923 "Lighting Control Devices."
4. Intercom and program systems specified in Section 275123 "Intercommunications and Program Systems."
5. Access control system specified in Section 281300 "Access Control."
6. Fire alarm system specified in Section 283111 "Digital, Addressable Fire-Alarm System."
7. Video surveillance system specified in Section 282300 "Video Surveillance."

C. 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 Communication, Signal, Control, and Low-Voltage Power Lines: Listed and labeled by a qualified testing agency for compliance with NFPA 731.

D. Intrusion Detection Units: Listed and labeled by a qualified testing agency for compliance with UL 639.

E. Interference Protection: Components shall be unaffected by radiated RFI and electrical induction of 15 V/m over a frequency range of 10 to 10,000 MHz and conducted interference signals up to 0.25-V rms injected into power supply lines at 10 to 10,000 MHz.

F. Tamper Protection: Tamper switches on detection devices, control units, annunciators, pull boxes, junction boxes, cabinets, and other system components shall initiate a tamper-alarm signal when unit is opened or partially disassembled and when entering conductors are cut or disconnected. Master control-unit alarm display shall identify tamper alarms and indicate locations.

G. Self-Testing Devices: Automatically test themselves periodically, but not less than once per hour, to verify normal device functioning and alarm initiation capability. Devices transmit test failure to master control unit.

H. Antimasking Devices: Automatically check operation continuously or at intervals of a minute or less, and use signal-processing logic to detect blocking, masking, jamming, tampering, or other operational dysfunction. Devices transmit detection of operational dysfunction to master control unit as an alarm signal.

I. Addressable Devices: Transmitter and receivers shall communicate unique device identification and status reports to master control unit.

J. Remote-Controlled Devices: Individually and remotely adjustable for sensitivity and individually monitored at master control unit for calibration, sensitivity, and alarm condition.

2.3 ENCLOSURES

A. Interior Sensors: Enclosures that protect against dust, falling dirt, and dripping noncorrosive liquids.

B. Interior Electronics: NEMA 250, Type 12.

C. Exterior Electronics: NEMA 250, Type 4X, fiberglass.

D. Corrosion Resistant: NEMA 250, Type 4X, PVC.

E. Screw Covers: Where enclosures are readily accessible, secure with security fasteners of type appropriate for enclosure.

2.4 SECURE AND ACCESS DEVICES

A. Manufacturers: Subject to compliance with requirements, provide products by one (1) of the following:

1. Bosch Security Systems, Inc.
2. Digital Security Controls Ltd.; a business unit of Tyco Safety Products.
3. Edwards Signaling & Security Systems; part of GE Security.
4. Honeywell International Inc.; Honeywell Security.

B. Keypad and Display Module: Arranged for entering and executing commands for system-status changes and for displaying system-status and command-related data.

C. Key-Operated Switch: Change protected zone between secure and access conditions.

2.5 DOOR AND WINDOW SWITCHES

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

1. General Electric Company; GE Security, Inc.
2. Honeywell International Inc.; Honeywell Security.

B. Description: Balanced-magnetic switch, complying with UL 634, installed on frame with integral overcurrent device to limit current to 80 % of switch capacity. Bias magnet and

minimum of two encapsulated reed switches shall resist compromise from introduction of foreign magnetic fields.

C. Flush-Mounted Switches: Unobtrusive and flush with surface of door and window frame.

D. Overhead Door Switch: Balanced-magnetic type, listed for outdoor locations, and having door-mounted magnet and floor-mounted switch unit.

E. Remote Test: Simulate movement of actuating magnet from master control unit.

2.6 PIR SENSORS

A. Manufacturers: Subject to compliance with requirements, provide products by one (1) of the following:

1. Bosch Security Systems, Inc.
2. Digital Security Controls Ltd.; a business unit of Tyco Safety Products.
3. General Electric Company; GE Security, Inc.
4. Honeywell International Inc.; Honeywell Security.

B. Listed and labeled by a qualified testing agency for compliance with SIA PIR-01.

C. Description: Sensors detect intrusion by monitoring infrared wavelengths emitted from a human body within their protected zone and by being insensitive to general thermal variations.

1. Wall-Mounted Unit Maximum Detection Range: 125% of indicated distance for individual units and not less than fifty (50) feet.
2. Ceiling-Mounted Unit Spot-Detection Pattern: Full 360-degree conical.
3. Ceiling-Mounted Unit Pattern Size: Eighty four (84) inch diameter at floor level for units mounted ninety six (96) inches above floor; eighteen (18) foot diameter at floor level for units mounted twenty five (25) feet above floor.

D. Device Performance:

1. Sensitivity: Adjustable pattern coverage to detect a change in temperature of 2^0F or less, and standard-intruder movement within sensor's detection patterns at any speed between 0.3 to 7.5 fps across two adjacent segments of detector's field of view.
2. Test Indicator: LED test indicator that is not visible during normal operation. When visible, indicator shall light when sensor detects an intruder. Locate test enabling switch under sensor housing cover.
3. Remote Test: When initiated by master control unit, start a test sequence for each detector element that simulates standard-intruder movement within sensor's detection patterns, causing an alarm.

2.7 ACOUSTIC-TYPE, GLASS-BREAK SENSORS

A. Manufacturers: Subject to compliance with requirements, provide products by one (1) of the following:

1. Digital Security Controls Ltd.; a business unit of Tyco Safety Products.
2. General Electric Company; GE Security, Inc.
3. Honeywell International Inc.; Honeywell Security.

B. Listed and labeled by a qualified testing agency for compliance with SIA GB-01.

C. Device Performance: Detect unique, airborne acoustic energy spectrum caused by breaking glass.

1. Sensor Element: Microprocessor-based, digital device to detect breakage of plate, laminate, tempered, and wired glass while rejecting common causes of false alarms. Detection pattern shall be at least a twenty (20) foot range.
2. Hookup Cable: Factory installed, not less than seventy two (72) inches.
3. Activation Indicator: LED on sensor housing that light when responding to vibrations, remaining on until manually reset at sensor control unit or at master control unit.
4. Control Unit: Integral with sensor housing or in a separate assembly, locally adjustable by control under housing cover.
5. Glass-Break Simulator: A device to induce frequencies into protected glass pane that simulate breaking glass without causing damage to glass.

2.8 PIEZOELECTRIC-TYPE, GLASS-BREAK SENSORS

A. Manufacturers: Subject to compliance with requirements, provide products by one (1) of the following:

1. General Electric Company; GE Security, Inc.
2. Honeywell International Inc.; Honeywell Security.

B. Listed and labeled by a qualified testing agency for compliance with SIA GB-01.

C. Device Performance: Detect unique, high-frequency vibrations caused by breaking glass.

1. Sensor Element: Piezoelectric crystals in a housing; designed to mount directly to glass surface with adhesive provided by element manufacturer. Circular detection pattern, with at least a sixty (60) inch radius on a continuous glass pane. Sensor element shall not be larger than four (4) sq. in.
2. Hookup Cable: Factory installed, not less than seventy two (72) inches.
3. Activation Indicator: LED on sensor housing that light when responding to vibrations, remaining on until manually reset at sensor control unit or at master control unit.

4. Control Unit: Integral with sensor housing or in a separate assembly, locally adjustable by control under housing cover.
5. Glass-Break Simulator: A device to induce frequencies into protected glass pane that simulate breaking glass without causing damage to glass.

2.9 VIBRATION SENSORS

A. Manufacturers: Subject to compliance with requirements, provide products by one (1) of the following:

1. General Electric Company; GE Security, Inc.
2. Honeywell International Inc.; Honeywell Security.

B. Listed and labeled by a qualified testing agency for compliance with SIA GB-01.

C. Description: A sensor control unit and piezoelectric crystal sensor elements that are designed to be rigidly mounted to structure being protected.

D. Device Performance: Detects high-frequency vibrations generated by use of such tools as oxyacetylene torches, oxygen lances, high-speed drills and saws, and explosives that penetrate a structure while not responding to any other mechanical vibration.

1. Circular detection pattern, with at least a seventy two (72) inch radius on protected structure.
2. Hookup Cable: Factory installed, not less than seventy two (72) inches.
3. Control Unit: Integral with sensor housing or in a separate assembly, locally adjustable by control under housing cover.
4. Glass-Break Simulator: A device to induce frequencies to protected glass pane that simulate breaking glass without causing damage to glass.

2.10 PHOTOELECTRIC SENSORS

A. Manufacturers: Subject to compliance with requirements, provide products by one (1) of the following:

1. General Electric Company; GE Security, Inc.
2. Honeywell International Inc.; Honeywell Security.

B. Device Performance: Detect an interruption of a pulsed, infrared, light beam that links transmitter and receiver.

1. Sensitivity: Detect standard-intruder movement within sensor's detection patterns at any speed of less than 7.5 fps though the beam. Allow installation of multiple sensors within same protected zone that will not interfere with each other.

2. Activation Indicator: LED indicator shall not be visible during normal operation. Indicator shall light when sensor detects a standard intruder. Locate test enabling switch under sensor housing cover.
3. Remote Test: When initiated by master control unit, start a test sequence for each detector element that simulates standard-intruder movement within sensor's detection patterns, causing an alarm.

2.11 MICROWAVE-PIR DUAL-TECHNOLOGY SENSORS

A. Manufacturers: Subject to compliance with requirements, provide products by one (1) of the following:

1. General Electric Company; GE Security, Inc.
2. Honeywell International Inc.; Honeywell Security.

B. Description: Single unit combining a sensor that detects changes in microwave signals and a PIR sensor that detects changes in ambient level of infrared emissions caused by standard-intruder movement within detection pattern.

C. Listed and labeled by a qualified testing agency for compliance with SIA PIR-01.

D. Device Performance: An alarm is transmitted when either sensor detects a standard intruder within a period of three (3) seconds to eight (8) seconds from when the other sensor detects a standard intruder.

1. Minimum Detection Pattern: A room twenty (20) feet by thirty (30) feet.
2. PIR Sensor Sensitivity: Adjustable pattern coverage to detect a change in temperature of 2^0F or less, and standard-intruder movement within sensor's detection patterns at any speed between 0.3 to 7.5 fps across two adjacent segments of detector's field of view.
3. Microwave Sensor Sensitivity: Adjustable, able to detect standard-intruder movement within sensor's detection pattern at any speed between 0.3 to 7.5 fps. Sensor sensitivity adjustments shall be accessible only when sensor housing is removed, and sensors shall comply with 47 CFR 15.
4. Activation Indicator: LED indicator shall not be visible during normal operation. Indicator shall light when sensor detects a standard intruder. Locate test enabling switch under sensor housing cover.
5. Remote Test: When initiated by master control unit, start a test sequence for each detector element that simulates standard-intruder movement within sensor's detection patterns, causing an alarm.

2.12 DURESS-ALARM SWITCHES

A. Manufacturers: Subject to compliance with requirements, provide products by one (1) of the following:

1. General Electric Company; GE Security, Inc.
2. Honeywell International Inc.; Honeywell Security.
3. Visonic Inc.

B. Description: A switch with a shroud over the activating lever that allows an individual to covertly send a duress signal to master control unit, with no visible or audible indication when activated. Switch shall lock in activated position until reset with a key.

1. Minimum Switch Rating: Fifty thousand (50,000) operations.
2. Foot Rail: Foot activated, floor mounting.
3. Push Button: Finger activated, suitable for mounting on horizontal or vertical surface.

2.13 VIDEO MOTION SENSORS (INTERIOR)

A. Manufacturers: Subject to compliance with requirements, provide products by one (1) of the following:

1. General Electric Company; GE Security, Inc.
2. Visonic Inc.

B. Device Performance: Detect changes in video signal within a user-defined protected zone. Provide an alarm output for each video input.

1. Detect movement within protected zone of standard intruders wearing clothing with a reflectivity that differs from that of background scene by a factor of two (2). Reject all other changes in video signal.
2. Modular design that allows for expansion or modification of number of inputs.
3. Controls:

   a. Number of detection zones.
   b. Size of detection zones.
   c. Sensitivity of detection of each protected zone.

4. Mounting: Standard nineteen (19) inch rack as described in EIA/ECA 310-E.

2.14 MASTER CONTROL UNIT

A. Manufacturers: Subject to compliance with requirements, provide products by one (1) of the following:
1. Honeywell International Inc.; Honeywell Security.

B. Provide Honeywell Vista, 250 RP Control UON.

C. Description: Supervise sensors and detection subsystems and their connecting communication links, status control (secure or access) of sensors and detector subsystems, activation of alarms and supervisory and trouble signals, and other indicated functions.

1. 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.
2. 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.
4. Control circuits for operation of mechanical equipment in response to an alarm.

D. Construction: Freestanding equipment rack, modular, with separate and independent alarm and supervisory system modules. Alarm-initiating protected zone boards shall be plug-in cards. Arrangements that require removal of field wiring for module replacement are unacceptable.

E. Comply with UL 609.

F. Console Controls and Displays: Arranged for interface between human operator at master 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: LCD, two line(s) of eighty (80) characters, minimum.
2. Keypad: Arranged to permit entry and execution of programming, display, and control commands.
3. Control-Unit Network: Automatic communication of alarm, status changes, commands, and other communications required for system operation. Communication shall return to normal after partial or total network interruption such as power loss or transient event. Total or partial signaling network failures shall identify the failure and record the failure at the annunciator display and at the system printer.
4. Field Device Network: Communicate between the control unit and field devices of the system. Communications shall consist of alarm, network status, and status and control of field-mounted processors. Each field-mounted device shall be interrogated during each interrogation cycle.
5. Operator Controls: Manual switches and push-to-test buttons that do not require a key to operate. Prevent resetting of alarm, supervisory, or trouble signals while alarm or trouble condition persists. Include the following:

a. Acknowledge alarm.
b. Silence alarm.
c. System reset.
d. LED test.

6. Timing Unit: Solid state, programmable, three hundred sixty five (365) days.
7. Confirmation: Relays, contactors, and other control devices shall have auxiliary contacts that provide confirmation signals to system for their on or off status. Software shall interpret such signals, display equipment status, and initiate failure signals.
8. Alarm Indication: Audible signal sounds and a plain-language identification of the protected zone addressable detector originating the alarm appears on LED display at master control unit. $ds~Annunciator panel alarm light and audible tone identify protected zone signaling an alarm.
9. Alarm activation sounds a bell or siren and strobe.

G. Protected Zones: Quantity of alarm and supervisory zones as indicated, with capacity for expanding number of protected zones by a minimum of 25%.

H. Power Supply Circuits: Master control units shall provide power for remote power-consuming detection devices. Circuit capacity shall be adequate for at least a 25% increase in load.

I. UPS: UPS shall be sized to provide a minimum of six (6) hours of master control-unit operation.

J. Cabinet: Lockable, steel enclosure arranged so operations required for testing, normal operation, and maintenance are performed from front of enclosure. If more than a single cabinet is required to form a complete control unit, provide exactly matching modular enclosures. Accommodate all components and allow ample gutter space for field wiring. Identify each enclosure by an engraved, laminated, phenolic-resin nameplate. Lettering on enclosure nameplate shall not be less than 1 inch high. Identify, with permanent labels, individual components and modules within cabinets.

K. Transmission to Monitoring Station: A communications device to automatically transmit alarm, supervisory, and trouble signals to the monitoring station, operating over a standard voice grade telephone leased line. Comply with UL 1635.

L. 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.

2.15 AUDIBLE AND VISUAL ALARM DEVICES

A. Manufacturers: Subject to compliance with requirements, provide products by one (1) of the following:

1. Cooper Wheelock.
2. Edwards Signaling & Security Systems; part of GE Security.
3. Honeywell International Inc.; Honeywell Security.

B. Bell: Ten (10) inches in diameter, rated to produce a minimum sound output of 84 dB at ten (10) feet from master control unit.

1. Enclosure: Weather-resistant steel box equipped with tamper switches on cover and on back of box.

C. Siren: 30-W speaker with siren driver, rated to produce a minimum sound output of 103 dB at ten (10) feet from master control unit.

1. Enclosure: Weather-resistant steel box with tamper switches on cover and on back of box.

D. Strobe: Xenon light complying with UL 1638, with a clear polycarbonate lens.

1. Light Output: One hundred fifteen (115) cd, minimum.
2. Flash Rate: Sixty (60) per minute.

2.16 SECURITY FASTENERS

A. Operable only by tools produced for use on specific type of fastener by fastener manufacturer or other licensed fabricator. Drive system type, head style, material, and protective coating as required for assembly, installation, and strength.

B. Manufacturers: Subject to compliance with requirements, provide products by one (1) of the following:

1. Acument Global Technologies North America.
2. Safety Socket LLC.
3. Tamper-Pruf Screws.

C. Drive System Types: Pinned Torx-Plus or pinned hex (Allen).

D. Socket Flat Countersunk Head Fasteners:

1. Heat-treated alloy steel, ASTM F 835.
2. Stainless steel, ASTM F 879, Group 1 CW.

E. Socket Button Head Fasteners:

1. Heat-treated alloy steel, ASTM F 835.
2. Stainless steel, ASTM F 879, Group 1 CW.

F. Socket Head Cap Fasteners:

1. Heat-treated alloy steel, ASTM A 574.
2. Stainless steel, ASTM F 837, Group 1 CW.

G. Protective Coatings for Heat-Treated Alloy Steel:

1. Zinc chromate, ASTM F 1135, Grade 3 or Grade 4, for exterior applications and interior applications where indicated.
2. Zinc phosphate with oil, ASTM F 1137, Grade I, or black oxide unless otherwise indicated.

PART 3 - EXECUTION

3.1 EXAMINATION

A. Examine substrates, areas, and conditions, with Installer present, for compliance with requirements for installation tolerances and other conditions affecting performance of intrusion detection.

B. Examine roughing-in for embedded and built-in anchors to verify actual locations of intrusion detection connections before intrusion detection installation.

C. Prepare written report, endorsed by Installer, listing conditions detrimental to performance of intrusion detection.

D. Inspect built-in and cast-in anchor installations, before installing intrusion detection, to verify that anchor installations comply with requirements. Prepare inspection reports.

1. Remove and replace anchors where inspections indicate that they do not comply with requirements. Reinspect after repairs or replacements are made.
2. Perform additional inspections to determine compliance of replaced or additional anchor installations. Prepare inspection reports.

E. For material whose orientation is critical for its performance as a ballistic barrier, verify installation orientation.

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

3.2 SYSTEM INTEGRATION

A. Integrate intrusion detection system with the following systems and equipment:

1. Electronic door hardware.

2. Elevators.
3. Network lighting controls.
4. Intercommunications and program systems.
5. Public address and mass notification systems.
6. Access control.
7. Fire-alarm system.
8. Video surveillance.

3.3 SYSTEM INSTALLATION

A. Comply with UL 681 and NFPA 731.

B. Equipment Mounting: Install master control unit on finished floor with tops of cabinets not more than seventy two (72) inches above the finished floor.

C. Install wall-mounted equipment, with tops of cabinets not more than seventy two (72) inches above the finished floor.

D. Connecting to Existing Equipment:

1. Connect new equipment to existing control panel in existing part of the building.
2. Connect new equipment to existing monitoring equipment at the Supervising Station.
3. Expand, modify, and supplement existing control and monitoring equipment as necessary to extend existing control and monitoring functions to the new points. New components shall be capable of merging with existing configuration without degrading the performance of either system.

E. Security Fasteners: Where accessible to inmates, install intrusion detection components using security fasteners with head style appropriate for fabrication requirements, strength, and finish of adjacent materials except that a maximum of two different sets of tools shall be required to operate security fasteners for Project.

3.4 WIRING INSTALLATION

A. Wiring Method: Install wiring in metal raceways according to Section 260533 "Raceways and Boxes for Electrical Systems." Conceal raceway except in unfinished spaces and as indicated. Minimum conduit size shall be one half (1/2) inch. Control and data transmission wiring shall not share conduit with other building wiring systems.

B. Wiring Method: Install wiring in metal raceways according to Section 260533 "Raceways and Boxes for Electrical Systems," except in accessible indoor ceiling spaces and in interior hollow gypsum board partitions where cable may be used. Conceal raceways and wiring except in unfinished spaces and as indicated. Minimum conduit size shall be one

half (1/2) inch. Control and data transmission wiring shall not share conduit with other building wiring systems.

C. Wiring Method: Cable, concealed in accessible ceilings, walls, and floors when possible.

D. Wiring within Enclosures: Bundle, lace, and train conductors to terminal points. Use lacing bars and distribution spools. Separate power-limited and non-power-limited conductors as recommended in writing by manufacturer. Install conductors parallel with or at right angles to sides and back of enclosure. Connect conductors that are terminated, spliced, or interrupted in any enclosure associated with intrusion system to terminal blocks. Mark each terminal according to system's wiring diagrams. Make all connections with approved crimp-on terminal spade lugs, pressure-type terminal blocks, or plug connectors.

E. Wires and Cables:

1. Conductors: Size as recommended in writing by system manufacturer unless otherwise indicated.
2. 120-V Power Wiring: Install according to Section 260519 "Low-Voltage Electrical Power Conductors and Cables" unless otherwise indicated.
3. Control and Signal Transmission Conductors: Install unshielded, twisted-pair cable unless otherwise indicated or if manufacturer recommends shielded cable, according to Section 280513 "Conductors and Cables for Electronic Safety and Security."
4. Data and Television Signal Transmission Cables: Install according to Section 280513 "Conductors and Cables for Electronic Safety and Security."

F. Splices, Taps, and Terminations: Make connections only on numbered terminal strips in junction, pull, and outlet boxes; terminal cabinets; and equipment enclosures.

G. Install power supplies and other auxiliary components for detection devices at control units unless otherwise indicated or required by manufacturer. Do not install such items near devices they serve.

H. Identify components with engraved, laminated-plastic or metal nameplate for master control unit and each terminal cabinet, mounted with corrosion-resistant screws. Nameplates and label products are specified in Section 260553 "Identification for Electrical Systems."

3.5 IDENTIFICATION

A. Identify system components, wiring, cabling, and terminals. Comply with identification requirements in Section 260553 "Identification for Electrical Systems."

B. Install instructions frame in a location visible from master control unit.

3.6 GROUNDING

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

B. Ground system components and conductor and cable shields to eliminate shock hazard and to minimize ground loops, common-mode returns, noise pickup, cross talk, and other impairments.

3.7 FIELD QUALITY CONTROL

A. Pretesting: After installation, align, adjust, and balance system and perform complete pretesting to determine compliance of system with requirements in the Contract Documents. Correct deficiencies observed in pretesting. Replace malfunctioning or damaged items with new ones and retest until satisfactory performance and conditions are achieved. Prepare forms for systematic recording of acceptance test results.

1. Report of Pretesting: After pretesting is complete, provide a letter certifying that installation is complete and fully operable; include names and titles of witnesses to preliminary tests.

B. Testing Agency: Engage a qualified testing agency to perform tests and inspections.

C. Manufacturer's Field Service: Engage a factory-authorized service representative to inspect, test, and adjust components, assemblies, and equipment installations, including connections.

D. 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.

E. Tests and Inspections: Comply with provisions in NFPA 731, Ch. 9, "Testing and Inspections."

1. Inspection: Verify that units and controls are properly labeled and interconnecting wires and terminals are identified.
2. Test Methods: Intrusion detection systems and other systems and equipment that are associated with detection and accessory equipment shall be tested according to Table "Test Methods" and Table "Test Methods of Initiating Devices."

F. Documentation: Comply with provisions in NFPA 731, Ch. 4, "Documentation."

G. Tag all equipment, stations, and other components for which tests have been satisfactorily completed.

H. The Contractor shall demonstrate the functionality of the System upon completion of installation, documenting the result of all tests and providing these results to the Owner. The System shall be tested in accordance with the following:

1. The Contractor shall conduct a complete inspection and test of all installed equipment. This includes testing and verifying connection to equipment of other Divisions.

2. The Contractor shall provide staff to test all devices and all operational features of the System for witness by the Owner's representative and the Authority having jurisdiction. The Contractor shall provide two-way radio communications to assist in the testing. All testing must be witnessed by the owner's representative, prior to acceptance.
3. The testing and certification shall take place as follows:

   a. System shall be tested in conjunction with the manufacturer's representative.

   b. All deficiencies noted in the above test shall be corrected.
   c. Test results shall be submitted to the consultant or owner's representative.
   d. System test witnessed by owner's representative and correction of any deficiencies noted.
   e. The owner's representative shall accept the System.
   f. System test shall be witnessed by the Authority having Jurisdiction, and any deficiencies that are noted shall be corrected.

4. A letter of certification shall be provided to indicate that the tests have been performed and all devices are operational.

3.8 ADJUSTING

A. Occupancy Adjustments: When requested within twelve (12) months of date of Substantial Completion, provide on-site assistance in adjusting system to suit actual occupied conditions. Provide up to three visits to Project during other-than-normal occupancy hours for this purpose. Visits for this purpose shall be in addition to any required by warranty.

3.9 DEMONSTRATION

A. Train Owner's maintenance personnel to adjust, operate, and maintain the intrusion detection system. Comply with documentation provisions in NFPA 731, Ch. 4, "Documentation and User Training."

END OF SECTION 281600