

SECTION 281300 - SECURITY & ACCESS CONTROL SYSTEM

PART 1 - GENERAL

1.1 RELATED DOCUMENTS:

- A. Contract drawings and general provisions of the Contract, including General and Supplementary Conditions apply to this Section and shall be considered a part of this section and shall have the same force as if specified herein full.

1.2 DESCRIPTION:

- A. This project includes the supply, installation, programming, testing, and commissioning of a complete and fully operational Access Control System (ACS). Reference contract drawings and specifications for specific requirements. Hardwired electric door hardware is being provided and installed by the General Contractor. Loading of software, programming, and training will be performed by the Security Contractor. The ACS will monitor controlled doors for forced entry and be held open independently of the Intrusion Detection System.
- B. The electronic security contractor shall be responsible for all cabling, hardware, and miscellaneous equipment required to provide a fully functional commercial ACS.
- C. The electronic security contractor shall coordinate with the owner for each system's requirements for notifying security personnel or proper authorities.
- D. The Security Contractor shall provide, install, and customize all Client software. The Security Contractor must coordinate with the owner's IT Support for network connection and device addresses. All configuration and programming shall be the responsibility of the Security Contractor.

1.3 QUALITY ASSURANCE:

- A. Industry Referenced Standards. The following specifications, certifications, and standards are incorporated into and become a part of this Specification by reference.
 - 1. FCC compliance
 - 2. UL compliance
 - 3. NEC compliance
 - 4. ISO 9001 Certification
 - 5. ISO 140001 Certification
 - 6. FIPS-140-2 Certification

1.4 INSTALLER'S QUALIFICATIONS:

- A. Firm with at least 5 years of successful application, installation, and testing experience on specified systems and equipment. All supervisors and installers assigned to the installation of this system or any of its components shall have factory certification from each equipment manufacturer that they are qualified to install and test the provided products. All installers assigned to the installation of this system

or any of its components shall have a minimum of 3 years of experience in the installation of the specified equipment.

- B. Security Contractor must be a Certified Installer of the manufacturer of the Card Access System. Certification must be provided in the form of a letter from the ACS Manufacturer or training certificate indicating that the Security Contractor (not an employee) is a Certified Installer.
- C. The Security Contractor must be licensed in the State of Georgia as a Low Voltage Telecommunications or Low Voltage class certification.
- D. The responsibilities of the Security Contractor shall include but not be limited to the following:
 - 1. Shop drawings on all Card Access Systems and equipment.
 - 2. Installation of all new Card Access Systems and equipment as documented in the drawings and specifications.
 - 3. Set up, configuration, programming, and commissioning of all ACS workstations and the ACS server.
 - 4. Coordination with the owner to establish a list of common card reader/door names. Then programming all card reader/door names into the ACS.
 - 5. Wire and wiring termination for all Card Access Systems and equipment.
 - 6. Testing and check-out of all Card Access Systems and equipment.
 - 7. Training for all Card Access Systems and equipment.
 - 8. Warranty for all Card Access Systems and equipment with the exception of OWNER PROVIDED items.
 - 9. As-Built drawings, operations, and maintenance for the complete Card Access System.

1.5 SUBMITALS:

- A. Product Data: Submit the manufacturer's technical product data, including specifications and installation instructions, for each type of system equipment. Include drawings, which contain complete wiring and schematic diagrams and other details required to demonstrate that the system has been coordinated and will function properly as a system. Drawings shall include floor plan layouts of devices, components, vertical riser diagrams, equipment rack details, elevation drawings of equipment racks, sizes and types of all cables and conduits.
- B. Test Plan: Contractor shall submit a test plan which defines the tests required to ensure that the system meets technical, operational, and performance specifications, 15 days prior to the proposed test date. Owner/User must approve the test plan before the start of any testing. The test plan shall identify the capabilities and functions to be tested and include detailed instructions for the setup and execution of each test and procedure for evaluation and documentation of the results.
- C. It is the responsibility of the contractor to meet with the appropriate owner's Representative to compare the placement and installation of proper devices with the drawings and specifications. A 100% device-by-device test will be conducted by the vendor under the supervision of the owner's representative. Punch lists will be developed at that time and furnished to the contractor. All punch list items must be corrected and verified prior to acceptance of the system.

- D. Written documentation, in the form of a Letter from the Manufacturer or Certificate must be provided with a Submittal Package demonstrating that the Security Contractor is a certified and authorized Dealer and Installer of the approved Access Control System.

1.6 DRAWINGS:

- A. The Contract Drawings indicate the arrangement of the access control system equipment. Coordinate installation of equipment with the structural, mechanical, and electrical equipment and access thereto. Coordination installation of recessed equipment with concealed ductwork and piping, and wall thickness.
- B. All raceways required for the ACS System are not shown on the Contract Drawings. The Security Contractor must coordinate with the Electrical Contractor to ensure that conduit is provided as necessary to complete the installation of the Access Control System.
- C. AutoCAD drawings (floor plans only) in electronic DWG format shall be provided to the Security Contractor for the production of shop drawings and As-built drawings. The Security Contractor is totally responsible for the conversion, if necessary, of the electronic files to whatever in house CAD program the Security Contractor utilizes for the production of the as-built drawings.

1.7 FINAL CLOSEOUT DOCUMENTS:

- A. Original content, taken directly from the Contract Drawings, shall be refused. As-built drawings must show true as-built conditions and must be prepared using the Contractors title block, symbols and notes explaining specific details of the installation.
- B. The following are minimum requirements for close-out documents. Final payment shall not be issued until all requirements have been met.
 - 1. Prior to project closeout, provide two (2) sets of complete data on equipment used for this project. This data shall be in bound form and shall include 11 x 17 as-built drawings.
 - 2. All as-built drawings shall include system interconnection diagrams with major components identified and the number and type of interconnecting conductors. Drawings must show actual as-built conditions and point-to-point diagrams.
 - 3. Two (2) full-size sets of as-built drawings shall be provided in hard copy format.
 - 4. As built drawings shall be provided on an external USB hard drive and in electronic format (PDF and AutoCAD - DWG).
 - 5. Two (2) bound copies with Table of Contents and tabs of the Operating and Maintenance (O & M) Manuals shall be provided to the Owner.
 - 6. Certificate or Letter of Acceptance from OWNER.
 - 7. Training Sign-In Sheets for each training session.
 - 8. A total of two (2) copies of the training video shall be provided.
 - 9. Document and provide two (2) copies of the network configuration (such as a list of IP addresses and the devices the addresses belong to, a line diagram demonstrating network topology, etc.).

- C. Completed (meaning open items have been cleared) Construction Observation Report.
- D. Security Contractor Warranty Form / Letter providing a detailed description of warranty provisions, duration of warranty period, start date, end date, and other information as described by these specifications.
- E. Manufacturer's Warranty Form / Letter providing a detailed description of warranty provisions, duration, and start date.
- F. All related documents required for substantial completion, system acceptance, and final payments.

1.8 ACCEPTABLE MANUFACTURERS:

- A. Reference products section of specifications for acceptable manufacturers.

1.9 WARRANTY:

- A. The Security Contractor shall warrant the Access Control System (ACS) for one year from date of start-up against defects in equipment or workmanship. Failed equipment shall be replaced by the Security Contractor at no cost to the owner. The owner's personnel may perform initial trouble investigation, but replacement of failed equipment and escalated problem support will be handled by the Security Contractor.
- B. The Security Contractor shall provide a Warranty Letter indicating the start date of the warranty. The Warranty Letter shall also provide contact information (Company name, Service Supervisor's name and phone numbers for normal working hours and Emergency Service request). The warranty period will not start until the Warranty Letter has been reviewed, approved, and agreed upon by the owner. Also, the Warranty Letter shall provide a brief description of the items covered under the warranty.

1.10 DESCRIPTION:

- A. The work included under this section of the specifications consists of the installation of a complete ACS System. Provide all labor, equipment, materials, and supervision to install, calibrate, adjust, document, and test the total system as required herein and on the drawings.
- B. The contractor shall provide all documentation and shall perform all duties involved in obtaining work permits as required to complete the project. All permits shall be within the associated city or jurisdiction.
- C. The work shall consist of the installation of a complete ACS System consisting essentially of, but not limited to, the following major components:
 - 1. Programming the existing Access Control System Server (Enterprise)
 - 2. Control Panels, control modules and keypads
 - 3. Network Base ACS Controllers
 - 4. Reader Interface Modules
 - 5. Input / Output Modules

6. Field Peripheral devices (i.e., iClass Contact-less Smart Cards, Smart Card Readers, Bio-metric Readers, PIR-passive infrared motion sensors, duress switches, sounders, electric door hardware, etc.)
 7. All required configuration and programming of the existing Server and Client Application and Operating System Software
 8. Power supplies with battery back-up & Uninterruptable Power Supplies (UPS)
 9. Network Switches and Patch Panels
- D. The new ACS shall be a network-based system using conventional WAN/LAN network connections.

1.11 SYSTEM OVERVIEW:

- A. The ACS shall be able to provide Access Control, Identity Management, Alarm Management, and other functionality in a single fully integrated ACS.
- B. The ACS shall carry FIPS-140-2 certification of appropriate parts of its communication encryption infrastructure, and the manufacturer shall provide the NIST certificate number confirming certification. Systems that do not carry FIPS-140-2 certification shall not be acceptable.
- C. The existing ACS Client and Server software shall be used in conjunction with intelligent controllers to provide a distributed access control and alarm monitoring system. In the event of a communications failure between the host server and the field controllers, the controllers shall continue to make local access control decisions and save all transactions in memory until communications are restored. At that time the controller shall upload all stored transactions to the server.
- D. The ACS shall seamlessly integrate the functions of access control, and alarm monitoring. All licenses for all these items added to the renovated area shall be included as part of the base price of the proposal, and not as extra-cost options.

1.12 ACCESS CONTROL SYSTEM REQUIREMENTS:

- A. The ACS will provide the option of using either conventional modular door controllers which enable between 2 and 16 doors to be housed within one steel enclosure or alternatively using Edge Network Controllers supporting PoE+.
- B. The ACS intelligent database controller shall support a minimum of 20,000 cardholders with expansion capabilities of up to 1,000,000 cardholders.
- C. The ACS intelligent database controller shall support a minimum of 12,000 offline transactions and at least 65,000 transaction storage at the panel.
- D. The ACS hardware shall be comprised of modular components that connect over standard interfaces to one another. There shall be a database storage and processing module (DBU), and once data has been downloaded to the DBU it shall locally make access control decisions. Access granted or denied decisions shall be made in under 0.5 seconds.
- E. The DBU shall store firmware in non-volatile flash memory to allow for convenient updates through a firmware update application. The DBU shall store the cardholder and configuration database information in battery-backed memory so that loss of primary power will not cause the loss of the database.

- F. The ACS hardware shall be capable of expansion via 2-, 4-, and 8- door controllers (DC). Door controllers shall support one or more input/output module expansion cards that require no additional addressing and provide 8 monitored input points or 8 auxiliary output points.
- G. The DBU shall support configurations that include: 16 card readers, 96 monitored input points, or 96 auxiliary output points.
- H. There shall be an intelligent controller option to provide control of 8 readers/doors from a single circuit board (communications, memory, CPU, and reader/door functions integrated) with an available 8-reader/door add-on to provide a 16-door controller from two circuit boards. The 8-door controller shall provide an integrated on-board RS-232 interface and shall have provisions for modular expandable memory.
- I. Each supplied card reader shall be continuously monitored for tamper (reader removed from backing plate or reader removed from wall). Tamper detection switch must be part of the reader and fit entirely within the reader housing. The use of external tamper switches shall not be acceptable. This requirement does not apply to biometric reader devices.
- J. To ensure synchronization of the distributed controllers' databases with a region's main database, an internal checking process shall be provided within each controller. In the event of corruption of a controller's local database then it shall be able to detect this condition and automatically request the relevant data to be downloaded from its local server. This action shall not require Operator intervention. The system shall continue to provide access control functionality during this re-synchronization process.
- K. The ACS shall support various reader technologies and provide data from card presentations or biometric authentications through a door control unit (DC) that includes the electrical interface to the reader as well as inputs for door sensors and form C relays for outputs.
- L. The Door Control (DC) shall support Wiegand communications to the reader. In order to provide higher levels of security, the DC shall also support bi-directional, supervised communications to the reader.
- M. The ACS hardware (except retrofit controllers and connected legacy devices) shall support all of the following options for supervision of the monitored input points:
 - 1. 2-state supervision – in which only secured, and alarm state are indicated.
 - 2. 3-state supervision – in which the input state can be secure, alarm or open circuit.
 - 3. 4-state supervision – supports secure, alarm, short circuit, and open circuit states.
 - 4. 6-state supervision – supports secure, alarm, short or open circuit for the sensor in addition to tamper alarm and tamper short circuit states.
- N. All electronic circuits supplied shall be mounted on standoffs inside the manufacturer-supplied enclosures. All such enclosures must include a key lock on a removable hinged door and must include a tamper switch to detect when the door is opened. Systems without key locking of enclosure doors or without doors which are both hinged and removable shall not be acceptable.

- O. All electronic circuits supplied for the ACS shall be powered by 18-20VAC through supplied 120VAC to 20VAC molded case, fully insulated isolating transformers. The transformer shall be mountable inside the supplied enclosure or separately.

1.13 COMMUNICATIONS

A. Network Communications

- 1. Field panels shall have the ability to communicate with its server or (for very large systems) its communications PC over the local or wide area network. This shall be achieved by the addition of a network interface option module (except in the case of controllers with a pre-installed network interface card [NIC]). The network interface shall support a minimum of "100 base TX" communications speed.
- 2. The network interface shall support encryption utilizing AES 128 or AES 256 algorithms.
- 3. Field panel models should be available to allow chains of connected panels to be created where the first panel is directly connected to the network and a minimum of 30 additional intelligent field panels daisy-chained together such that they communicate back to the single network interface.

B. Hardwired Communications

- 1. The field panels shall be located conveniently to the access and monitor points that they control and shall be interconnected in a chain configuration to the server or a serial port of a convenient communications PC on the system.
- 2. The system shall support a minimum of 31 intelligent field panels daisy-chained together such that they communicate back to a single serial communications port at the server/communications PC.

PART 2 - PRODUCTS

2.1 MATERIALS:

- A. Materials or equipment specified by manufacturer's name shall be provided, unless approval of other manufacturers is listed in addendum to these Specifications. Any materials or equipment approved in addendum shall function the same as the equipment specified.

2.2 ACCESS CONTROL SYSTEM (ACS):

- A. The project shall standardize on one (1) unified ACS and video surveillance system manufacturer so that Facility Maintenance and System Administrators may be adequately trained to maintain, operate, and program the system. The approved manufacturers include:
 - 1. Continental Access
- B. The Security Contractor shall be required to be a Certified Installer of the Security & Access Control System and be fully trained to implement the system on an enterprise level.

2.3 DOOR CONTROL PANEL

- A. The ACS control panels shall be intelligent and fully stand-alone processor capable, making all local access control decisions without host server dependency. Control panels shall support and provide the following:
1. UL listed under UL 294 and UL 1076; FCC Part 15 and CE compliant.
 2. Direct on-board support for industry standard RS232, RS422, Dial-up modem AT command set, and 10/100Mb Ethernet communications interfaces to ACS hosting server or operator workstations.
 3. Support for redundant communications to ACS hosting server or operator workstations; primary communications via 10/100Mb Ethernet with automatic switchover to secondary communications via dial-up modem when detecting network failure.
 4. The ACS shall use DES/3DES encryption algorithms for the protocol between network-based control.
 5. RS232 and RS422 communications ports for cascading/clustering multiple control panels via a single communications port interface to ACS hosting server or operator workstations.
 6. Flashable memory support for facilitating remote firmware updates from ACS host server and operator workstations; control panels shall remain on-line and operational during firmware update process.
 7. Persistent Memory: The database memory downloaded to the ACS control panel shall be written to FLASH memory for permanent retention during the event of total power failure. The database shall automatically recover after power is restored without requiring any connection to the ACS server.
 8. Control panel cabinet shall be of an industrial grade enclosure with knockouts for field wiring and have a key-locked and tamper protected door.
 9. Low voltage power supply with uninterruptible battery backup allowing continued operations for a minimum of 2 hours at full load.
- B. Control Panel Interfaces: The ACS control panels shall support on board and/or expansion interface boards for access control readers, and input/output control. Control panels shall support and provide the following as required:
1. Access Control Reader Interfaces:
 - a. Shall support hard-wired connections to readers, including power and communications. Connections shall be supported at a minimum distance of 2,000ft. (610m) utilizing 22AWG 2-pair shielded and unshielded cabling.
 - b. Shall support supervision, monitoring, and processing of the following:
 2. Reader tamper and communications.
 3. Status changes from locally wired door sensor and request to exit device.
 - a. Shall support card only and card-plus-keypad style readers of the following technologies:
 - 1) Proximity.
 - 2) Smart Card.
 - 3) Magnetic Stripe.
 - 4) Wiegand.
 - 5) Barcode.

- 6) BaFe Touch.
- 7) Biometrics.
- b. Input / Output Point Interfaces:
- c. Shall support 4-State supervised alarm inputs.
- d. Shall support relay and TTL level output points.

- C. Required access control panels shall be the Continental Access CICIP2800 Super-Speed with backup batteries sized for 4 hours of continuous operation.

2.4 WORKSTATIONS:

- A. The Security Contractor is responsible for configuring and programming the existing ACS Client software application. Then all programming and configuration necessary to ensure a completely operational workstation that is connected to the existing ACS Server.
- B. The Security Contractor is responsible for coordinating with the owner's IT Support for the installation of all required software.

2.5 BUILDING CARD READERS:

- A. The ACS System shall provide the ability to support HID multiCLASS readers.
- B. Each card reader shall have a low profile, rugged, weatherized polycarbonate sealed enclosure with multi-color LEDs and sounder for access granted and access denied indications. Each reader shall be mountable indoor or outdoor. All readers mounted externally shall be environmentally sealed. Card reader shall be one of the models stated below based on mounting requirements.
 - 1. HID model Signo20 card reader with Bluetooth capability – mullion mounted (typically utilized for store front style entry / exit doors).
 - 2. HID model Signo40 card reader with Bluetooth capability – single gang back box mounted (typically utilized for interior doors).
 - 3. HID model Signo40K card reader with keypad with Bluetooth capability – single gang back box mounted (typically utilized for interior doors that require a higher level of security such as card plus pin).
- C. Security Contractor to coordinate color with Owner.
- D. The acceptable manufacturer for card readers shall be HID Corporation. No substitutions allowed.

2.6 NETWORK SWITCH:

- A. Security Contractor shall coordinate requirements for network switch ports to be provided by Grady Hospital's IT Departments.

2.7 ACCESS CARDS:

- A. A quantity of 100(100) HID iClass, Smart Cards shall be provided with the hospital's facility code.
 - 1. The card shall function at 13.56 MHz.
 - 2. The card shall function as a 125kHz proximity card.

3. The card shall have a read range of up to 4 inches.
4. The card shall be compatible with HID multiCLASS card readers.
5. The card shall have an ISO MIFARE microprocessor.
6. The card shall have 2k bits of memory.
7. The card shall be ISO14443 compliant.

2.8 ELECTRONIC LOCKING TECHNOLOGY – PROVIDED BY DIVISION 8

- A. The security contractor shall coordinate with the door hardware contractor on the placement of required electronic locking hardware. The door contractor will provide and install all electric locking hardware with the associated line voltage power supplies, unless otherwise noted in drawings. The security contractor will provide all necessary wire and cable, low voltage power supplies, terminate all connections, and shall interface this equipment with the integrated security system.

2.9 D.C. POWER SUPPLY PANEL

- A. Provide low voltage power supply units associated with Local Interface Units and Door Control Panels and as required to provide both 12 and 24 volts regulated, filtered D.C. power for locking controls, D.C. locks and signal devices. Output power shall be both 12 and 24 volt D.C. with an ampere rating not less than 150% of load imposed on power supply under most severe conditions of load. D.C. output shall be fused. Output voltage shall be regulated within plus or minus 5% from no load to full load. Power supply shall be UL listed. The power supply also shall have the ability to individually select fire alarm disconnect for any of the supplied outputs.
- B. Power supplies shall be connected to the campus security network via a network interface module. Module will facilitate status monitoring of power status, output current draw, temperature, output voltage and battery status. The module shall have the capability to notify personnel via e-mail should any issues arise with the given power supply.
- C. Contractor shall provide the following for each panel:
 1. All cables shall be labeled at each termination.
 2. As-built drawings shall be left inside the panel.
 3. Wire management shall be installed throughout each panel for cable routing.
 4. Panel locks shall be re-keyed per owner requirements.
 5. Enclosure tamper switches must be installed for all enclosures and monitored as an individual alarm point.
- D. Power Supplies shall be manufactured by Altronix. Contractor shall provide UL600ULACM power supply with batter backup.

2.10 DURESS ALARM

- A. Duress alarm devices shall be a supervised, latching devices, capable of mounting in both vertical and horizontal positions. Wall mount, under desk/counter, etc.) Provide duress alarm hardware as indicated in the Contract Drawings.

- B. Duress alarm device shall consist of an ABS fire-retardant plastic housing with internal electrical circuitry and magnetic reed contacts with an actuating lever for activation. The device shall be configured for latching operation so that once activated the actuating lever must be reset AND a reset signal provided by the ACM.
- C. Duress button shall be a United Security Products, Model # HUB2A.

2.11 INTRUSION DETECTION SYSTEM (IDS)

- A. Each building's control panel shall be the main point of programming, monitoring, accessing, securing, and troubleshooting the IDS. Refer to American National Standards Institute (ANSI) CP-01 Control Panel Standard-Features for False Alarm Reduction.
- B. The Control panel shall utilize a direct wire download interface module and Ethernet/serial converter to communicate with the IDS system via Ethernet TCP/IP connection for integration. Ethernet/Serial converter shall be certified by the manufacturer for use with the IDS and the application.
- C. The Control panel shall utilize a Multifunctional Keypad, Input, and Output Modules for expansion of alarm zones, interfacing with additional security subsystems, programming, monitoring, and controlling the IDS.
- D. The Control panel shall meet or exceed the following minimum functional requirements for programming outputs, system response, and user interface:
 - 1. Programming Outputs:
 - a. 2 Amps (A) alarm power at 12 VDC
 - b. 1.4 A auxiliary power at 12 VDC
 - c. Four alarm output patterns
 - d. Programmable bell test
 - e. Programmable bell shut-off timer.
 - 2. System response:
 - a. Selectable point response time
 - b. Cross point capability
 - c. Alarm verification
 - d. Watch mode
 - e. Scheduled events arm, disarm, bypass, and un-bypass points, control relays, and control authority levels.
 - 3. User Interface:
 - a. Supervises up to eight command points (e.g. Up to 8 unsupervised keypads can be used)
 - b. Provides custom keypad text.
 - c. Addresses full function command menu including custom functions.
 - d. Allows user authority by defined area and 16-character name.
 - e. Provides for 14 custom authority control levels allowing user's authority to change, add, delete passcodes, disarm, bypass points, and start system tests.
- E. The Control panel shall meet or exceed the following technical characteristics:

Input Voltage via 110 VAC or 220 VAC Step-down Transformer	16 or 18 VAC
Operating Voltage	12 VDC
Output Voltage	12 VDC @ 2 A max

Direct Hardwire Zones	7
Partitions	8
Multifunctional Keypads	16 (2 per partition)
Communications Port	RJ-11

- F. A multifunctional keypad shall be utilized as a user interface for arming, disarming, monitoring, troubleshooting, and programming the alarm control panel.
- G. The control panel shall have a communications port that will allow for communications with a computer for programming, monitoring, and troubleshooting purposes. The communications port will be, at a minimum, an RJ-11 or better.
- H. The control panel will have a systems success probability of 95% or better, and shall include the following success considerations:
 - 1. False Alarm: Shall not exceed one (1) false alarm per 30 days per sensor zone.
 - 2. Nuisance Alarm: Shall not exceed a rate of one (1) alarm per seven (7) days per zone within the first 60 days after installation and acceptance. Sensor adjustments will be made and then shall not exceed one (1) alarm per 30 days.
- I. The Control Panel will be able to detect either a line fault or power loss for all supervised data cables.
- J. Honeywell Vista 20 security control panel, Model # V2060KT1

2.12 INTRUSION ALARM CONTROL PANEL

- A. Keypads shall be a multi-line, 32-character English language display for complete zone identification and system status. The keypad shall be wall mounted.
- B. Honeywell alpha numeric keypad, Model #6160

2.13 MOTION DETECTORS

- A. Motion detection devices shall utilize dual technology signal processing with both PIR and microwave signals processed through the unit's microcontroller. Units shall support multiple functions, including concurrent diagnostics, digital fluorescent light interference filter, digital adaptive microwave threshold, adaptive baselines, and bidirectional temperature compensation.
- B. The detector shall provide the detection, signal processing, alarm relay, and operating power circuitry in the same enclosure; and shall provide an alarm relay actuation upon the detection of an intruder moving into or through its protection pattern. Each detector shall feature a single-piece electronics board whose circuitry is specifically designed for the detector and mounted to a housing with the cover is secured. The case shall include wiring knockouts for installation.
- C. Wall mount Motion Detection devices shall contain a front mounted, dual-purpose lens that shall focus received infrared energy onto the sensor. The lens shall be capable of providing wide angle detection patterns of up to 40ft x 56ft.
- D. Wall mount Motion detectors shall be typical to Honeywell Model #DT8050V units or approved equal.
- E. Ceiling mounted Motion Detection devices shall contain a spherical lens capable of providing a 360-degree detection area of up to 25 FT when mounted at 8'-0" above

the finished floor. The ceiling mounted motion detector shall be Visonic, 360 deg, ceiling mount motion detector: model #DUO240, 360 degree dual-tech.

2.14 GLASS BREAK DETECTORS

- A. Glass break detectors are to be wall or ceiling mounted based on the required range of sensors as noted by the manufacturer. Mount on the wall where ceilings are beyond 10 feet in height.
- B. Glass break detectors will use multiple technologies to detect breaking glass.
- C. Detectors shall be typical of Glass break detectors are to be wall or ceiling mounted based on the required range of sensors as noted by the manufacturer. Mount on the wall where ceilings are beyond 10 feet in height.
- D. Glass break detectors will use multiple technologies to detect breaking glass.
- E. Detectors shall be typical of Honeywell Flexguard Glass break detector, Model #FG1625F series units.

2.15 CELLULAR COMMUNICATOR

- A. Cellular communicator shall be UL listed for Commercial Business applications.
- B. Cellular communicators shall have the capability to serve as either primary or backup alarm communications and shall allow full data reporting from the security panel.
- C. Verizon, LTE M style cellular alarm communicator, Model # LTEM-XV unit.

2.16 IDS SECURITY AUXILIARY POWER SUPPLY

- A. Auxiliary Power Supply with enclosure, transformer, and backup battery.
 - 1. Input: 6VDC from TP1640 plug-in transformer
 - 2. Output:
 - a. 6VDC or 12VDC selectable output.
 - b. 2.5A continuous supply current.
 - c. Filtered and electronically regulated output.
 - d. Short circuit and thermal overload protection.
 - 3. Battery Backup:
 - a. Built-in charger for sealed lead acid or gel type batteries.
 - b. Automatic switch over to stand-by battery when AC fails.
 - c. Battery short circuit protection (circuit breaker).
 - 4. Altronix Model #SMP3ET

2.17 SURGE PROTECTION

- A. All security components installed outdoors or exposed to lightning shall be provided with surge and lightning protection. Provide UL listed multi-stage protection on all low voltage and signal transmission lines. All 120 VAC surge suppression devices shall be EDCO HSP121BT-1RU or an approved equivalent. For low voltage connections, provide FAS-1 surge suppressors manufactured by EDCO or an approved equivalent. For RS-485 or RS-422 connections, provide PC642C-008LC with base PCB1B manufactured by EDCO or an approved equivalent.

2.18 DOOR POSITION SWITCH CONTACTS:

- A. Provide high security type balanced magnetic contacts which are shown on the contract drawing.
- B. Surface mounted: Door contacts shall be provided with supervised loop and shall have a flexible armored cable with total encapsulation to protect against moisture. Door contact shall have anodized aluminum finish, with stainless steel flexible cable. Door contacts shall be UL Listed and be warrantied for two years. Door contact for surface mount swing door locations shall be Honeywell 7939BR or approved equal. Door contacts for surface mount roll-up door locations shall be Honeywell 958M series or approved equal. Door contacts for recessed mounted swing or sliding door locations to serve the Access Control and Intrusion Detection systems shall be Edwards 1076D Double Pole, Double Throw or equal.

2.19 EMERGENCY EXIT BUTTON

- A. Security Contractor shall provide Emergency Exit push buttons in locations indicated on the Contract Drawings.
- B. Emergency Pushbuttons shall have the following features:
 - 1. Fit in a single gang box.
 - 2. Have a 2" square button with the text "Push To Exit"
 - 3. Thirty (30) second relock delay, fixed.
 - 4. Reactivation – pushing the switch at any time restarts the timer cycle.
 - 5. Failsafe mode releases lock when power to the switch is lost.
 - 6. Illuminated push button.
- C. Provided Securitron EEB2 or LV Engineer approved equal.

2.20 REQUEST TO EXIT DEVICES:

- A. Provide request to exit (REX) devices as indicated on the Contract Drawings.
- B. Mount wall mounted type passive infrared motion detectors (PIR) used as (REX) devices, to effect automatic unlocking of electric door operators and locks via ACS System's LIU's and/or DCP's. (PIR) devices shall have wide angle, long range lenses (adjustable) to detect motion of personnel desiring to exit through the door. Coordinate exact field mounting location to provide best operation of (PIR) type (REX) device. (PIR) device shall operate at 9.0 to 16.0 VDC and have form-C output contacts rated at minimum 24 VDC/0.5 amps.
- C. Provide Bosh Model # DS150I Request-to-Exit Motion Sensor.

2.21 EMERGENCY EGRESS DEVICES

- A. Emergency egress devices shall be required at any door provided with magnetic locking hardware and where electronic locking hardware prevents exiting through a designated emergency path of egress.
- B. Emergency egress devices shall be mechanically operated device to provide direct interruption of locking hardware without interfacing with electronic controllers or relays.

- C. Emergency egress devices for this project shall be integrated with the electronic hardware and shall be provided and installed by the Door Hardware Contractor.
- D. It shall be the responsibility of the Security Contractor to notify the design team and Owner of any access controlled door that does not meet emergency egress requirements.

2.22 ELECTRIFIED DOOR HARDWARE:

- A. All electrified door hardware shall be provided and installed by the General Contractor.
- B. The Contractor shall be responsible for connecting and terminating all electrified door hardware and associated devices to the new ACS System.

2.23 VIDEO ENTRY INTERCOM SYSTEM

- A. IP Video Master Station shall be a SIP-enabled desk station and provide support for basic telephony features including hold, transfer, call waiting, and call history without the use of a PBX.
- B. The station shall support at least 30 IP call stations without the use of a PBX and shall meet the following additional requirements.
 - 1. Power Source: Power over Ethernet (802.3af)
 - 2. Network interface 10Base-T / 100 Base-TX Ethernet (RJ-45).
 - 3. Compatible IP protocols: IPv4, IPv6, TCP, UDP, SIP, HTTP, HTTPS, MJPEG, RTSP, RTP, RTCP, IGMP, MLD, SMTP, DHCP, NTP, DNS.
 - 4. Communications: Hands-Free (VOX), Push-to-Talk, or handset (full-duplex).
 - 5. 7-inch LCD Video Display Screen
 - 6. Door Release Button: Programmable Form C dry contact, 24V AC/CD, 1A.
 - 7. Wall or desk mounting with included stand and bracket.
 - 8. Video Stream: ONVIF Profile S.
 - 9. Camera:
 - a. 1/3-inch color CMOS, 1.23 MP.
- C. The acceptable model shall be Aiphone IX-MV-HB, color black with a handset.
- D. IP Intercom Sub-Station
- E. The IP Sub-Station shall consist of an outdoor rated vandal resist and, ADA compliant, speakerphone configured for single button operation, and integrated ONVIF compliant Camera.
 - 1. Power Source: Power over Ethernet (802.3af)
 - 2. Network interface 10Base-T / 100 Base-TX Ethernet (RJ-45).
 - 3. Compatible IP protocols: IPv4, IPv6, TCP, UDP, SIP, HTTP, HTTPS, MJPEG, RTSP, RTP, RTCP, IGMP, MLD, SMTP, DHCP, NTP, DNS.
 - 4. Door Release: Programmable Form C dry contact, 24V AC/CD, 1A.
 - 5. Video Stream: ONVIF Profile S.

- F. IP Sub-station shall be suitable for installation in outdoor environments and constructed for installation in vandal-resistant outdoor environments and rated for IP65 installation.
- G. IP Sub-Station shall include the ability to call at least six (6) intercom master stations.
- H. IP Sub-Station shall function using standard POE Ethernet connectivity for power and communications and shall additionally support standard SIP protocol.
- I. IP Sub-Station shall include a wide-angle megapixel IP camera.
- J. Flush mount IP Sub-Stations shall be provided with a custom backbox.
- K. The acceptable model shall be the Aiphone model IX-DVF with custom surface backbox SBX-IXDV30 30° angle box if the camera view requires the intercom station to be angled.

2.24 OUTDOOR RATED ALARM STROBE

- A. Provide outdoor rated alarm strobe – audible/visual signal where they are shown on the contract drawings.
- B. Alarm sounder strobe shall be equal to Federal Signal Model #SLM500 with a shallow base or equal. Provide with backbox and mounting plate for outdoor installation.
- C. Strobe color to be selected by the owner. Options include amber, blue, clear, green, or red.

2.25 Contractor to wire to Security System and provide the appropriate power supply. SYSTEM WIRING

- A. Card reader connection cable shall be of a type specified by the manufacturer of the ACS System. Cable must meet minimum NEC requirements for Class 2 wiring.
- B. Power wiring for electrified door hardware shall not be smaller than No. 18 THWN or XHHW.
- C. All wiring systems shall use solid copper conductors except where flexibility is required. Stranded conductors shall be acceptable only where all terminations can be made to crimp type screw lug.
- D. All wiring systems shall be color-coded so that each conductor for individual lock set is of a distinctive color. All wiring shall be in accordance with the manufacturers' written recommendations. All cabling/wiring shall be submitted in a detailed spreadsheet including cut sheets and samples to the Owner prior to any installation.
- E. All conductors within junction boxes, pull boxes, and equipment cabinets shall be grouped and laced with nylon tie straps with identification tabs, for individual lock sets.

PART 3 - EXECUTION

3.1 INSTALLATION:

- A. System components and appurtenances shall be installed in accordance with NFPA 70, manufacturer's instructions, and as shown. Necessary interconnections, services, and adjustments required for a complete and operable signal distribution

system shall be provided. Penetrations in fire-rated construction shall be fire-stopped in accordance with contract documents. Conduits and raceways shall be installed in accordance with the National Electric Code (NEC). Cables shall not be installed in the same cable tray, utility pole compartment, or floor trench compartment with AC power cables. Metal conduits shall not be continuous between buildings. Security Contractor to provide ground isolation between buildings by breaking continuous copper cabling and metal conduit runs.

B. Surge Protection:

1. All copper cables and conductors which serve as control, power, or data conductors shall have surge protection devices installed at each end that complies with electrical and security specifications.
2. Protect all video and data equipment from surges induced on all control, power and data cables. All copper cables and conductors which serve as control, power, or data conductors shall have surge protection circuits installed at each end that meet the IEEE 472 surge withstand capability test. Fuses shall not be used for surge protection.

C. The Access Control System shall be provided with a local interface with the Fire Alarm System to effect automatic unlocking of all doors controlled by the ACS System during Fire alarm conditions.

D. See Part 1 for programming requirements. Contractor will be required to fully customize the security & access control system with the following minimum features:

E. Graphic maps with active icons

F. Video surveillance and Intercom and emergency call system integration. Camera call-up from intercom calls and security events shall be a requirement.

G. Integration with existing HR databases.

H. Security system schedules

I. All functions described in specification section 1.12 - Access Control System Requirements

3.2 WIRING SYSTEMS:

A. Protect all communication and data equipment against surge induced on all control, sensor and data cables. All cables and conductors which serve as control, sensor, or data conductors shall have surge protection circuits installed at each end that meet the IEEE 472 surge withstand capability test and the electrical transient tests established in UL365. Fuses shall not be used for surge protection.

B. The work under this section of the specifications includes the installation of all wiring for the electrified door hardware. The actual connections to the electrified hardware and the access control system shall be done under this section of the specifications. It is the responsibility of the Security Contractor to coordinate all electrical requirements and connections of the electrified hardware.

3.3 CARD READER AND DOOR CONTROL PANELS:

A. Mount card reader sensors at a height of 46" AFF to center, unless shown otherwise. Mount card readers securely to the mounting surfaces and provide weather caulking around exterior mounted readers.

- B. Mount door control panels where shown on the contract drawings or where required to provide a completely operational system. All door panels must incorporate a minimum of 4 hours battery back for micro-processors as well as electrified door hardware.

3.4 ACCESS CONTROL SYSTEM CABLE AND TESTING:

- A. The manufacturer's technical representatives shall certify in writing that the systems are installed in compliance with the manufacturer's recommendations, comply with the requirements of the Contract Documents, and are operating correctly. These written certifications shall be submitted to the Architect and shall signify that the total security and communication system is operational and ready for substantial completion testing by the Architect.
- B. At substantial completion but prior to Final Inspection, the Security Contractor shall conduct operational testing to ensure that all systems are functioning as properly, all devices are powered up and are communicating with their associated head end equipment. The Security Contractor shall provide all personnel, equipment, instrumentation, and communication equipment and shall include the cost of operational testing in the Base Bid.
- C. After operational testing is completed by the Security Contractor, the Security Contractor shall coordinate a Date and Time for Final Inspection and Acceptance Testing with the Architect and the owner. The Security Contractor shall provide all personnel, equipment, instrumentation, and communication equipment and shall include the cost of Final Inspection and Acceptance Testing in the Base Bid. If upon arrival at the site, the Architect and OWNER find a System Server / Workstation non-operational or unable to perform system functions due to incomplete programming or more than five (5) field devices not functioning or connected to their associated head-end, a false start shall be declared by the Architect. This will result in an ADD SERVICE CHARGE of eight (8) hours at the Architect's current billing rate, submitted to the owner by the Architect. The owner will in turn back charge this cost to the Security Contractor
- D. At substantial completion of the electronic systems, testing shall be conducted by the Security Contractor as directed by the Architect. The Security Contractor shall provide all personnel, equipment, instrumentation, and communication equipment and shall include the cost of final acceptance testing in the base Contract.
- E. All newly installed Category 6 shall be tested. Each cabling permanent link or channel shall be tested and certified. Each pair of permanent links or channel shall be tested. The permanent link measurement is recommended although the entire channel may be tested. The entire channel includes the patch cables at the workstation end of the permanent link to the patch cables at the patch panel end.
 - 1. Each outlet must pass the following parameters for category 6 as described in ANSI/TIA/EIA-568-B.2-1: wire map, length, insertion loss, NEXT, Power Sum NEXT, ELFEXT, Power Sum ELFEXT, Return Loss, Propagation Delay, and Delay Skew.
 - 2. All tests shall be favorable, no *PASS, *FAIL or FAIL results shall be accepted.
 - 3. All test results shall be turned over to the owner in both electronic files and in hard copy.
- F. All newly installed Fiber Optic cable shall be tested. Optical fiber (backbone) cables shall be 100% tested for attenuation and length. Testing shall be performed with an

optical power meter and light source. The cable length shall be recorded using an OTDR, optical length test measurement device or sequential cable measurement markings. Attenuation shall be tested at 850 nm and at 1300 nm for multimode fiber cable. All test results shall be turned over to the owner in both paper and electronic format. Each strand shall not exceed a level of: 3.5 dB/km of attenuation for 850 nm and 1.5 dB/km of attenuation for 1300 nm

1. Each strand shall be tested and the following information be turned over to the owner
 - a. From point to point
 - b. Fiber I.D. label number
 - c. RX level
 - d. Attenuation total
 - e. Wave length
 - f. Reference level

3.5 TRAINING:

- A. The Contractor shall include in the base Contract all costs required to train owner operating and maintenance personnel in the use and maintenance of systems provided under this section of the Specifications. Training sessions shall be conducted by instructors that are certified by the manufacturer of the specific system.
- B. Sessions shall be conducted for not less than four-hour periods during normal working hours, i.e., Monday through Friday, 8:00 AM to 5:00 PM. Training session schedules shall conform to the requirements of; therefore, such schedules shall be submitted to the owner for approval not less than two weeks prior to the training session. All training sessions shall be video-recorded for future use. At the owner's discretion, provisions shall be made to allow up to 2 owner personnel to participate in final system check out of all systems.
- C. The Contractor shall keep a sign-in sheet during training. Sign-in sheet must be provided as part of close out documentation video recording provided on thumb drive shall be of professional quality both for video and audio and must be approved by the Owner/User: Provide two copies to Owner/User
- D. Time to be included in base Contracts for specific systems shall be as follows: ACS System Entirely 16 hours of Time.

END OF SECTION