ACCESS CONTROL SYSTEM – Appendix A

Part 1 – General

1.01 DESCRIPTION

1. Work Included:

    1. Under this Section, the Contractor is to provide an Access Control System (ACS), including all necessary components, conduits, and wiring as herein specified, as shown on the Drawings and as otherwise required for a complete and workable installation.

    2. Control panels shall be connected to an Owner provided security TCP/IP V-LAN network.

    3. The work includes providing all labor, materials, tools, equipment, and documentation required for a complete and working security management system as specified in this document.

2. Related Work Provided By Owner:

    1. The Contractor shall coordinate the work with the related work provided by the Owner including but not limited to the following:

        a. Network Connections

1.02 RELATED DOCUMENTS

A. Drawings and general provisions of Contract, including General and Supplementary General Conditions and other Division 01 specification sections, apply to this Section and to all Contractors, Subcontractors, or other persons supplying materials and/or labor, entering into the Project site and/or premises, directly, or indirectly.

B. The Specifications and Drawings are intended to be complementary. A particular section, paragraph or heading in a Division may not describe each and every detail concerning work to be done and materials to be furnished. The Drawings are diagrammatic and may not show all of the work required or all construction details. Dimensions are shown for critical areas only; all dimensions and actual placements are to be verified in the field. It is to be understood that the best trade practices of the Division will prevail. It remains the responsibility of the Contractor or Subcontractor to provide all items, equipment, construction, and services required to the proper execution and completion of the Work.

C. Reference listings are provided as a convenience to the Contractor or Subcontractor providing the Work of this Section and may not contain all the requirements affecting this Section. It remains the responsibility of the Contractor or Subcontractor to locate and comply with all requirements of the Contract Documents.

D. All related specification sections shall be used in conjunction with this section.

1.03 QUALITY ASSURANCE

A. Qualifications: The manufacturer/supplier shall meet all of the following criteria:

1. Shall be a manufacturer regularly engaged in the manufacture and assembly of access control systems a minimum of five (5) continuous years.

2. Shall be the authorized distributor or full service dealer of the access control system.

3. Shall have an office staffed with factory trained technicians, fully capable of engineering, supervising installation, system start-up, providing Owner training and supervising of both hardware and software for the access control system.

1.04 SUBMITTALS

A. General:

1. Prior to obtaining any material in connection with this Section, submit the following information for review.

a. Block diagrams of the proposed system and interconnection wiring diagrams showing all connections required between system components.

b. A materials list with names of manufacturers, model numbers, and technical information on all equipment proposed. Product technical information sheets for each principal component in the proposed system. Include wire/cable specifications and wire/cable marking material.

c. A complete operations manual for the system products being supplied.

1.05 WARRANTY

A. General:

1. All equipment and system shall be warranted against defects in material and workmanship for a period of two (2) years from the date of startup. Warranty coverage shall include parts, labor, travel, expenses, and labor to remove/reinstall all products. The warranty document shall be submitted with the Contractor's submittals and shall include details on inclusions and exclusions, deductibles, and availability of extended coverage options.

Part 2 – PRODUCTS

2.01 ACCEPTABLE MANUFACTURERS

A. Access Control System:

1. CBORD

B. Substitutions

1. No substitutions will be considered.

2.02 ACCESS CONTROL SYSTEM

A. System Description:

1. The ACS shall have the capability of an integral solution through the use of a per-planned suite of hardware and software modules for Access Control, Proprietary Alarm Monitoring, Video Badging, and Fire Alarm Annunciation.

2. This ACS shall provide a true multi-tasking, multi-terminal capability and shall be based upon Windows server operating system.

3. The ACS shall provide a high level of operating system security. Operator interaction shall be a Windows User Interface (GUI).

4. The ACS File Server shall be capable of communicating with multiple Workstations over Ethernet LAN using NetBEUI or TCP/IP.

5. The ACS shall be capable of controlling a minimum 250 doors.

6.

B. System Certifications:

1. The ACS shall be certified upon a 100% test completed by the technician assigned to the project.

C. Operator Interface:

1. The ACS software operator screens shall utilize all standard Windows style functions such as drop-down menus, radio buttons, check boxes, list boxes, etc. The ACS shall provide context sensitive help screen windows to insure the user's ability to receive on-line informational text pertinent to the task being performed. Access to these help screens shall be controlled with a dedicated function key or via the mouse and pull-down menus.

D. Computer Network:

1. The ACS system shall be based on the Windows server protocols NetBEUI or TCP/IP. Network limitations shall be determined by the Ethernet LAN topology used.

E. Historical Log:

1. The ACS shall allow event history to be written to a single or multiple locations on the system File Server and Workstations. The system shall have the capacity to store a minimum of 500,000 transactions. As the archive files reach a user programmable set value from 1 to 100% capacity, the system shall generate a "History Log Near Full" message. The system does not require that back-up archiving be accomplished when the message appears and will continue to archive additional events.

2. The system administrator shall either manually or on a pre-defined time schedule back-up archived data to an internally tape mechanism for off-line storage and later retrieval as required. The ACS software shall permit the formatting of this media in the background without requiring the operator to leave the ACS Operating Program.

F. System Status:

1. It shall be possible to query the status of any of the system's access control doors, input points, output points and alarm conditions. This status shall display the current state of the device in question at the time of query.

2.03 APPLICATION SOFTWARE

A. Cardholder Database:

1. The ACS shall provide an industry standard database management system application. The Cardholder database shall allow the designer to create, edit, and delete database tables and data entry as required. The system shall allow for the setup of a unique database structure to the customer's exact specifications.

2. The follow items shall be provided:

   a. A sample default database and screen design to help with initial start-up.

   b. All captions and controls will be available for dynamic viewing and rearranging.

   c. Up to five pages shall be available for placement of fields.

   d. Ability to drag-and-drop the data fields within each page.

   e. Alignment options shall be available to quickly line up all fields in any arrangement. Include badging camera, tripod, backdrop and all associated items to produce in-house video badges.

B. Security:

1. A password protection function shall allow the system administrator to assign access privileges and permit access to modules within the system. The password protection shall be linked with user status to permit or deny access to various system functions and levels.

2. The ACS shall allow the following maximum capacities within the definition of the Cardholder Database:

   a. Up to 5,000 Cardholder Records
   b. Up to 43 unique customer defined fields.
   c. Up to five pages for database fields.
   d. Up to 60 characters per field.
   e. Up to 16 Cardholder database partitions.
   f. Up to 16 look-up tables per partition.

C. Database Validation:

1. The ACS shall utilize the following Field Validation Methods for the manipulation and definition of data within each database field:

    a. Field is required – Data must be entered before exiting the screen.
    b. No Entry – Data may be viewed but not changed.
    c. Upper Case – All keystrokes are changed to uppercase.
    d. Invisible – The field exists but is not visible (the default for Generated Number fields).
    e. Numbers Only – Only numeric data (0-9) is allowed.
    f. Auto Fields – The system shall automatically add those fields require. The data elements themselves will not be modifiable by the system administrator to insure data integrity in the system.

D. Cardholder Configurations:

1. The system shall have the capability to support 5,000 cardholder files. The software shall be capable of having programmed with their standard assigned card code and/or PIN number format or they may be configured using their social security numbers plus up to three digits as a user identifier. Any cardholder shall be capable of having up to ten access levels actively assigned to their account.

2. Each cardholder assigned in the system shall be identified as either "Standard", "Visitor" or "Escort." The system shall also have the capability to assign a validity period to each cardholder having an Activation and Deactivation definable to: month-date-year.

3. Each cardholder database screen shall have a system-generated date/time stamp on each cardholder record. The ACS shall automatically enter the following data into each cardholders record based on cardholder usage:

    a. Last Edit by Operator
    b. Last Edited date/time
    c. Last date/time card was used
    d. Last reader giving valid access
    e. Last reader denying access
    f. Anti-Passback Status

4. The system software shall provide an Advanced Query capability of the cardholder database. This shall include search criteria: equal to, not equal to, greater than, greater than or equal to, less than, less than or equal to, like, is empty, is not empty, is between and, or, and not.

E. Cardholder Import/Export:

1. The ACS shall allow for the manual import of all or specific cardholder data over a network or via diskette or tape. Updates shall be by a repeat of the original import with updated files. Cardholder data, excluding the video image, shall be supplied to the ACS in one of the following formats: Bitmap, TIF, PICT, GIF, JPG.

2. The ACS shall allow for the manual export of all or specific cardholder data over a network or via diskette. Updates shall be by a repeat of the original export with updated files. The export of both database information and video images shall be available in the same forms as described above for import.

2.04 ACCESS CONTROL CONFIGURATION

A. Security:

1. The ACS shall provide a password protection scheme to prevent unauthorized individuals from entering the configuration application. Additionally, a second level of password authorization shall be provided to restrict what each individual may edit or display once inside the configuration application.

B. Descriptions:

1. The ACS shall allow text description of configuration items, such as doors, input points, etc.

2. The ACS shall allow the renaming of an existing title description without removing the sub-components of that configuration object. For example, rename a door from "Lobby" to "East Lobby" without any other changes to the configuration to support that title change.

C. Time Periods:

1. The ACS shall have a minimum of 256 time periods. Each time period shall have a minimum of 8 definable start and stop intervals.

D. Holidays:

1. The ACS shall allow the definition of up to 100 total holiday days. Each holiday shall override normal day activity. The ACS shall allow each holiday to span up to 31 days.

2. The ACS shall provide a mechanism for generating the actual date of the holiday based on the holiday requirements. The ACS shall provide for the following methods in defining a Holiday:

   a. The ACS shall allow the system administrator to define an "Annual" holiday one time, though the holiday is required yearly, Christmas for example. The administrator shall enter the Month and Day of the holiday. Thereafter, the ACS system shall automatically calculate the holiday date.

   b. The ACS shall allow the system administrator to define a "Relative" holiday one time, though the holiday shall be required yearly, Thanksgiving for example. The administrator shall enter the Month, Weekday, and Week Number of the holiday. Thereafter, the ACS system shall automatically calculate the holiday date.

   c. The ACS shall allow the system administrator to define an "Absolute" holiday one time only, Columbus Day Observed for example. The administrator shall enter the Month, Day, and Year. The ACS system shall only use this holiday one time.
   d. Sequences

e. Object tracing

E. Input Points:

1. The ACS shall support supervised and non-supervised connections of input devices for the purpose of monitoring locations. The ACS shall support the shunting or suppressing of inputs manually by authorized operators.

2. The ACS shall allow any input point to be part of a group of input points for the purpose of preventing viewing and control. This "grouping" shall allow specific buildings or floors to be partitioned from other users of the system.

F. Output Points:

1. The ACS shall support the activation/de-activation of outputs manually by authorized operators or automatically based on time of day.

2. The ACS shall allow any output point to be part of a group of output points for the purpose of preventing viewing and control. This "grouping" shall allow specific buildings or floors to be partitioned from other users of the system.

G. Input/Output Linking:

1. The ACS shall allow the definition of automatic linkage between input points and output points. The system shall allow each input point to be defined to automatically activate a single or group of outputs without operator intervention.

2. The ACS shall provide a means for reviewing which inputs are configured to activate which output points without leaving the configuration application.

H. Partitioning:

1. The ACS shall support the partitioning cardholder data within the security system. A partition is a distinct, separately managed group of data within the security database. The partitioning of a system and its points contains a single file server database which can be configured for unique control and display of system points that are relative to that location only.

I. Door Configuration:

1. The system shall support the assignment of the door unlock time and the door held open time. The door unlock time shall be used to unlock the door for a pre-defined time following a valid access or request to exit operation.

2. The ACS shall allow up to 300 seconds of time to be programmed for each door's unlock and door held open time. These functions shall be accomplished through the ACS software and no special hardware shall be required. Systems requiring additional components or timer modules or that require parameter adjustments for these functions to be set at their network controllers, data gathering panels or time modules and not through the system software will not be accepted.

3. Each door within the ACS system shall have the ability of being automatically unlocked based on the time of day. Any access controlled doors in the system shall have the ability to generate a local alarm output in the event of the door being forced or left open. The report of these events shall be time period definable.

4. Each door may utilize a request to exit input circuit to unlock the door without generating a forced door alarm condition. The ACS shall support the shunting of the door status switch when a request to exit device is enabled through the software. No additional hardware shall be required.

J. Download Manager:

1. Operator actions, system parameters and cardholder data programming and changes shall be capable of being intelligently downloaded to the system's network controllers. The download process shall be precisely controlled by an icon driven Download Manager which shall determine how, what, and when this shall be accomplished.

2. The operator using this manager shall be capable of choosing all or selected controllers, and involve specifically designated parts of the database e.g. time periods, access levels, cardholders, etc. The actual download process shall take place immediately based on a manual request or by an operator definable "Time Schedule". The ACS shall allow Time of Day downloading based on the following parameters:
   a. Specific day(s) of the week
   b. Specific day(s) of the month
   c. Specific time(s)

K. Event Messages:

1. The ACS shall provide a real-time status of the system activity depending on the current configurations of the ACS when the trigger point has been activated.

L. Event Message Routing:

1. The ACS shall allow each event message generated from the system to be routed to the following destinations:

   a. Historical Log(s): User defined directories on the hard drive used for real-time logging of event activity within the ACS.
   b. Printer(s): User defined printers that shall display the real-time occurrence of event activity within the ACS.
   c. Operator(s): User defined operator log on identifiers that shall display in real-time event messages within the ACS network.
   d. Workstation(s): User defined computer workstations that shall display in real-time the event messages within the ACS. All event activity shall be displayed on the workstation regardless of logged on operator.

2. The ACS shall allow all event messages to be configured to be routed to primary and auxiliary destinations by the time of day. If the time period is not enabled, the event message will not be routed.

M. Alarm Management:

1. Alarm priorities:
   a. The ACS shall provide an alarm priority queue from 1 to 99. Each alarm condition may be defined as 1 of the 99 priorities.

2. Break-through alarms:
   b. The ACS shall interrupt the current program being run and present the Alarm Display Screen automatically regardless of system activity when an alarm of a designated priority or higher is generated.

3. Auto launch alarms:
   c. The ACS shall allow alarms above a user selectable alarm priority (1-99) to automatically launch the Alarm Management application if it is not already open. This permits high priority alarms to be displayed regardless of current operator activity in another software application.

   d. CBORD CS Gold Software

2.05 MANAGEMENT REPORTS

A. The ACS shall provide a user friendly report management tool integral in design to the ACS system. The report generator shall allow reports to be generated from the following information storage locations:
   1. Archived History from any ACS workstation hard drive
   2. Archived History from a Network Backup
   3. Configuration data from the ACS File Server
   4. Configuration data from a Network Backup

B. The system shall provide a minimum of 5 report templates that provide the following real-time status information:
   1. Alarm Status
   2. Input Point Status
   3. Output Point Status
   4. Cardholder Region Occupancy Status
   5. Door Status

C. The system shall provide report templates that provide the following configuration information:
   1. ACS Workstation Configurations
   2. Time Period Configurations
   3. Holiday Configurations
   4. Input Point Configurations
   5. Output Point Configurations
   6. Access Levels Defined
   7. Door Access Level Configurations
   8. Cardholder Access Levels
   9. Cardholder Configurations
   10. Door Configurations

D. The ACS shall provide the capability to schedule reports to generate automatically to a file or printer location. The scheduler function shall allow reports to be printed:
   1. Daily
   2. Weekly
   3. Monthly

4. Any Time of Day

2.06 ACCESS CONTROL HARDWARE

A. Network Controller Hardware:

1. The system shall have distributed architecture and shall simultaneously support the interface of Intelligent System Controllers (ISC). Controllers shall have operating environment specifications to allow complete functionality at a temperature range of 0 to 50 deg. C and a relative humidity of 90% (non-condensing).

B. Access Control Panel (ACP):

1. The ACP shall be modular in design and have an ISA passive backplane bus with two reserved slots and 6 – (8) bit expansion slots.

2. The ACP shall be of a microprocessor-based design, with on-board time and date generation, and an on-board rechargeable battery to allow a minimum of 48 hours data and event buffer integrity.

3. The ACP shall utilize flash ROM for program storage. Program updates shall be made via download through the ACP service port and shall not require chip replacement.

4. Panels shall be 4-hour battery backed up with additional battery support time available within the same cabinet.

5. Each panel shall be capable of the following communications methods to the Security System:
   a. Direct line communication over 4 conductor, 22 AWG twisted shielded cable.

6. Each Access Control Panel may support up to (32) card readers. This baseline panel shall be responsible for the following:
   a. All non-host related access control monitoring and decision making events.
   b. Local Input/Output Linking
   c. Storage of up to 5,000 complete encoded card numbers, which shall be capable of optional expansion capacity to 5,000 card codes. Each cardholder record in the System Controller shall maintain the Access Level, Time Periods Door Restrictions and other pertinent decision making data.

7. Any Security System Host system which reverts to a degraded mode, using a facility code/site code or other lower security technique only shall not be accepted.

8. Each reader module shall be capable of interfacing with most major card reader technologies without the necessity of special interfacing. Systems requiring additional logic panels, interface cards or personality modules to provide this interface are not acceptable. These peripheral devices shall be connected to the reader module through snap-in plugs for servicing. The following reader technologies shall be supported:

a. Proximity
b. Magnetic Stripe
c. Wiegand
d. Bar Code
e. Keypad Only
f. Biometric
g. Proximity with integrated Keypad
h. Magnetic Stripe with Integrated Keypad

9. Each reader module shall be capable of accepting two keypads, or two readers or two keypad reader combinations. The reader module shall be capable of the following door control modes:
   a. Reader only
   b. Keypad only
   c. Reader and keypad
   d. Reader or keypad

10. Each reader module shall include the necessary electronics to support two door status contacts, two request to exit devices, and two door strike outputs. The door strike outputs shall control lock power and have a minimum contact rating of 2 Amps at 30 VDC.

11. Each reader module shall be supplied with additional operator definable input and output points. These auxiliary contacts shall be form "C" rated at 2A at 30 VDC. Each input point shall provide four conditions of status; normal, abnormal, cut and short. Each reader module shall be supplied with four additional closed loop/4 state supervised (selectable) inputs and two additional form C dry contact relay outputs.

12. Each input, including Door Switch and Request to Exit (REX) inputs shall have supervision capabilities and shall allow a minimum 500 foot, 22 gauge, TSP wire run to each input device.

C. Access Control Reader:

1) Manufacturer: Scheduled Manufacturer: Allegion aptiQ MT15. No substitutes will be accepted.

2) Requirements: Read Only Multi-technology Contactless reader
   a. Multi-technology contactless reader shall be read access control data from both 125 kHz and 13.56 MHz contactless smart cards and NFC-compatible. The multi-technology contactless reader shall be optimally designed for use in access control applications that require reading both 125 kHz Proximity and 13.56 MHz contactless smart cards

   b. Multi-technology contactless reader shall be configurable to read 13.56 MHz data simultaneously from the following cards (multiple credential support based on reader configuration): Secure support - Mifare DESFire EV1with PACSA, Mifare Classic, FIPS 201 PIV Credential.

   c. Multi-technology contactless reader shall provide the ability to read card access data stored in the secure access control sector/application area of the ISO 14443 XceedID MIFARE or MIFARE DESFire EV1 card.

   d. Dimensions: 5.1" x 3.25" x 0.83" (12.9 cm x 8.3 cm x 2.1cm)

e. Current requirements: 160 mA DC, 195 mA PEAK @ 12 VDC

3) The standard card shall be the size of a credit card and have a slot for a clip such that it will hang vertically. It shall be constructed of durable polycarbonate and be available with no artwork, multi colored custom artwork or with the system suppliers artwork. Allegion aptiQ (DESFire EV1).

D. Request to Exit Motion Detectors:

1. The Contractor shall provide request to exit motion (RTE) devices on each card reader controlled door to shunt the door position switch and allow free egress without initiating an alarm condition on the SMS. The RTE device shall be configured to activate for two seconds and automatically rest after that time to prevent extended shunting of the local alarm. DS 1501 Series.

a. PANEL INTERFACE MODULE

A. The Panel Interface Module (PIM) shall employ a spread spectrum 900MHz RF technology and shall support up to 16 doors within a 200’ radius. PIMS shall be centrally located to support door hardware in each facility.

B. The PIM shall employ a 128-bit encryption for security and shall be highly scalable.

Schlage PIM400-485

b. WIRELESS LOCKS – CYLINDRICAL TYPE

A. Access control contractor shall provide all wireless locks for each resident room. Contractor shall refer to Appendix B for details and hardware description and models.

c. MAGNETIC CONTACTS

A. Magnetic door contacts shall be provided for all exterior doors and windows and where indicated on the Drawings. Contacts shall mount on interior side of doors with no visible indication on the exterior. Contacts shall be suitable for use with the intended door or window. Double pole, double throw, GEIO76D or equivalent.

d. POWER SUPPLY

A. Door Locking Hardware Power Supplies:
1. It shall be the Integrator’s responsibility to provide the power supply capable of supporting the full power demands of the locking hardware as specified for a minimum of four (4) hours in the event of normal circuit power loss.
2. The locking hardware power supply shall be the Altronix AL1024ULACM or approved equal.
3. Provide battery backup for power supply. Altronix BT126 or approved equal.

Part 3 – Execution

3.01 DELIVERY, STORAGE AND HANDLING:

A. Installation Requirements:

1. Install system per the manufacturer's instructions.

2. Coordinate the operational compatibility of all locking devices not supplied by the Access Control manufacturer with the Access Control manufacturer.

3. If required by the Access Control manufacturer, the locking devices supplier shall include electronic suppression and be rated for continuous duty operation.

4. All locking device wiring shall be run separate from all other system wiring except wire specifically permitted by the Access Control supplier.

B. Testing and Commissioning:

1. The ACS supplier shall be responsible for final system hardware hook up and checkout prior to commissioning the system to the end user.

2. The ACS supplier shall be responsible for:
   a. Construction schedule of product and services
   b. Schedule of values
   c. Project Folder
   d. Routinely Scheduled Project Progress Management
   e. Factory Consultation Services

C. Training and Instruction:

1. Before the system is turned over to the owner, the manufacturer shall provide 5 days of system operations training at the project site using the customer's equipment for up to 10 of the owner's representatives meeting a minimum expected level of computer competence.

2. This training shall be conducted during normal business hours of the equipment supplier at a date and time of mutual convenience.
3. This training shall be conducted by a dedicated trainer employed full-time for the purpose by the manufacturer of the access control system. Representatives of a local dealer operation shall not be considered acceptable.

D. Software Support:

1. The ACS shall be supported by the manufacturer for no less than on year from date of system turnover.

E. Warranty:

1. The system shall be warranted for a period of 1 year from date of acceptance or first beneficial use, whichever occurs first. Written notification shall be sent to the owner stating the date this warranty period has started.

2. The equipment manufacturer shall make available to the owner a maintenance contract proposal to provide a minimum of two inspections and preventative tests per year.