SECTION 28 10 00

ACCESS CONTROL

PART 1 - GENERAL

1.1 DESCRIPTION

A. This Section covers access control and alarm monitoring systems (ACAMSs).

B. This Section covers wiring of electric door hardware provided under Division 8.

C. The ACAMS shall consist of workstations and a hierarchy of Mercury Access Controllers that communicate with the existing CBORD CS Access head-end servers utilizing Dartmouth's TCP/IP based Ethernet network.

1.2 RELATED SECTIONS

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

B. Additional related specification sections include:

1. Section 28 05 00, Common Work Results for Electronic Security.
2. Section 28 05 13, Conductors and Cables for Electronic Security.
3. Section 28 05 28, Pathways for Electronic Security.
4. Section 28 08 00, Commissioning of Electronic Security.
5. Section 28 20 00, Video Surveillance
6. Section 28 31 00, Intrusion Detection

1.3 QUALITY ASSURANCE

A. The access control system contractor, the contractor's supervisors, and technicians shall meet the qualifications as defined in Section 28 05 00, Common Work Results for Electronic Security Systems.

B. Qualifications of the Access Control System Contractor:

1. The access control system installation company shall have field office located within a 100-mile radius of the Project with a minimum of two permanently employed persons with current access control system certification directly responsible for the installation and ongoing maintenance of the project.
2. Installation of the access control system shall be provided by a person or persons having completed, as a minimum, the factory training recommended by the access control system manufacturer and have direct field experience in the installation of a minimum of 3 projects of similar scope and size within the past 5 years.
3. The access control system Project Manager or Project Supervisor shall have direct field experience in installing at least 3 access control systems projects of similar scope and size within the past 5 years.
4. Programming and configuration of the access control system shall be provided onsite by a person or persons having completed the access control system manufacturer's highest available certification program and have direct field experience in the programming and configuration of a minimum of 3 projects of similar scope and size within the past 5 years.

5. The access control system installation company shall be listed as an authorized dealer or business partner by CBORD and shall have been listed as such for at least 3 years.
6. For all major system database reconfigurations or upgrades the access control system contractor shall engage CBORD for onsite professional services for final programming and configuration of the system. The manufacturer shall certify that the systems are installed, programmed, and configured correctly and are complete and fully functional. Professional services shall be engaged for sufficient time to certify the system.

1.4 SUBMITTALS

A. See Section 28 05 00, Common Work Results for Electronic Security for additional requirements.

B. Action Submittals:

1. Product Data:

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

2. Shop Drawings:

a) Include site and floor plans indicating equipment locations. Plans shall include equipment identification and either direct references to wiring details for each specific installation and wiring condition or a schedule that references the same.
b) Wiring diagrams shall indicate proposed connections of equipment, model numbers, and designations for cables and termination points.
c) Provide elevations of cabinet or rack-mounted equipment, showing the location of all specified electronics and include enlarged, to scale plan (top), and front views.
d) Provide elevations of wall-mounted equipment, showing the location of all specified electronics and include enlarged, to scale plan (top), and front views.
e) Provide project specific manufacturer shop drawings of fabricated or modified units, if any.
f) Provide riser diagrams indicating components of the system and proposed cabling between these components.
g) Provide block diagrams indicating the proposed interface between the access control system and all other Enterprise Systems.
h) Provide detailed project specific mounting diagram for each type of device including raceway and back box requirements. These details shall be referenced in the floor plans or schedules.
i) Provide a detailed loading schedule for each access control system panel indicating card readers (by Door Number, card reader modules, and input/outputs (I/O) modules identifying each device connected to the I/O modules.

C. Informational Submittals:

1. Resumes of key personnel that document the qualifications required. Include certificate of training or certifications.
2. As required in Section 28 05 00, Common Work Results for Electronic Security.

D. Close-out Submittals:

1. Functional Test Reports: Provide a spreadsheet with all access control system devices and major components listed in the first column by device designator (e.g., door number) with each test parameter listed by name (or code) in the remaining columns.
2. Operations and Maintenance Documentation Package: As required in Section 28 05 00, Common Work Results for Electronic Security.
3. Instruction of Operating Personnel:
    a) The Security Systems Performance Verification Supervisor shall schedule, coordinate, assemble and deliver the documentation of the training required by this section.
    b) Obtain receipt from the Owner acknowledging completion of each item of instruction.
    c) See Section 28 05 00, Common Work Results for Electronic Security for additional requirements.

PART 2 - PRODUCTS

2.1 ACCESS CONTROL AND ALARM MONITORING SYSTEMS

A. General:

1. The system (hardware and software) shall support the quantity and types of devices specified herein and indicated in the Drawings.
2. Provide the quantity and type of software licenses required to support the readers, servers, and workstations at the levels of functionality specified herein, and as indicated on the Drawings.
3. Provide spare licenses and hardware to support 25% additional reader and IO capacity. The card reader controlling the door to the space housing the controller shall be connected to the MP1502 Controller. Reader boards shall be installed on the backplane only. All IO boards shall be installed on the inside of the door. When panels reach 75% capacity (12 doors for 16-door panels, 6 doors for 8-door panels) a new panel with an MP1502 Controller shall be provided.

2.2 APPLICATION SOFTWARE

A. General: the existing CBORD CS Access control system software shall serve as the database manager, controlling badge data, access rights, time schedules, multiple operation modes, and alarm point information.

1. Wireless Lockset Integration:
    a) The system shall support the integration of battery-operated wireless locksets with the security management system.
    b) Once a lockset is installed and registered with the controller, it shall function in the security application as an access-controlled door.
    c) It shall be possible to set configuration options for a wireless lockset to change its call-in and lockout behaviors.
    d) It shall be possible to specify special-use formats for access cards to be used with wireless locksets.
    e) The wireless lockset shall be able to send high priority events to the controller.
    f) The system shall support low battery monitoring of the wireless lockset.

g) It shall be possible to schedule an automatic unlock period for remote-lockset portals.

2. Graphic Maps:

a) The ACAMS shall support graphic maps and icons to be displayed on the operator workstation monitor.

b) The system shall support a programmable, color graphic map display that:

1) Shall be capable of showing the floor plan, the location of alarm devices, and alarm instructions for a facility.

2) Shall be centralized in the system configuration and displayed on the operators' workstations.

3) Shall allow various maps to be associated with different areas to create a hierarchy of maps.

4) Shall support graphic maps having a resolution of 1920 x 1080 pixels or greater.

c) The ACAMS shall allow an update of the drawings, without additional reconfiguration.

B. System Hardware:

1. Access control panels and interface boards:

a) Mercury MP1502 supports 4 readers, 8 inputs, and 4 outputs (preferred controller).

b) Mercury MP2500 Intelligent Controller board (No Onboard IO).

c) Mercury MR52 –S3 Reader interface board with 8 inputs and 6 outputs.

d) Mercury MR16IN-S3 interface panel supports 16 general-purpose input circuits.

e) Mercury MR16OUT-S3 interface panel provides 16 general purpose outputs as Form C relay contacts.

2. The access control panel shall be housed in a unified enclosure with a Life Safety Power M-Class PS with intelligent network monitoring.

3. Single Door (PoE+) Edge Network Controller:

a) The intelligent single door PoE edge network controller shall be the MP1501 supports 2 readers, 2 inputs, and 2 outputs provide access control processing, host functionality and power for a single door, including reader, lock, door status, request-to-exit device, and auxiliary sounder.

4. The controller shall support the Security Industry Association’s (SIA) Open Supervised Device Protocol (OSDP) compatible card readers.

5. Manufacturer: CBORD, with Mercury MP series hardware, and LifeSafety Power unified enclosure/power supply.

2.3 ACCESS CONTROL PERIPHERAL EQUIPMENT

A. Card and RFID Readers:

1. Card Readers:

a) Communication signals between the reader and the access control panel shall be encrypted and transmitted via RS-485 using the Security Industry Association’s Open Supervised Device Protocol (SIA 2012 OSDP).

b) Standard readers: HID 40.
c) Mullion style readers: HID 20.
d) Combination card plus PIN readers: HID 40K.
e) Combination mullion style card plus PIN readers: HID 20K.
f) Manufacturer and Model: HID Signo smart card readers.

2. Wireless Card Readers:
   a) Wireless card readers are not preferred, however, may be used in certain applications upon agreement with Dartmouth FO&M Access Control Shop.
   b) Communication signals between the reader and the access control panel shall be encrypted and transmitted via RS-485 using the Security Industry Association's Open Supervised Device Protocol (SIA 2012 OSDP).
   c) Networked wireless locks must NOT utilize the Dartmouth College WiFi network.
   d) Networked wireless locks and PIMs should be purchased through CBORD.
   e) Panel Interface Module Manufacturer and Model: Allegion PIM400.
   f) Lock Manufacturer and Model: Allegion AD400 Networked Wireless Lock.

2.4 POWER SUPPLY EQUIPMENT

A. Power Supplies:

1. Power supplies shall be provided in a unified NEMA 1 hinged enclosure with the control panels, reader interface boards and input/output boards.
2. Power supplies shall be Rated at 1.2 times the current draw for devices served. For door locking hardware, coordinate with the existing hardware for electrical power requirements.
3. Individually fused or PTC outputs to each device.
4. For lock power supplies provide input for connection to a UL listed fire alarm panel output, which upon initiation shall disconnect power to selectable lock outputs.
5. UL Class 2 rated outputs.
6. System Health and Performance Monitoring: Provide network interface module to allow monitoring of the following conditions and control functions:
   a) Total System Health: Faults, output draw, battery state and temperatures.
   b) Output Condition: Current draw, voltage level and output status.
   c) Battery Activity: Charging current, discharge level, time to service.
   d) Power History: AC outages, time stamped faults, and enclosure tampering
   e) Fire Alarm activation.
   f) Independent output control for remote reset functions
   g) Scheduled or manual battery checks
   h) AC loss or trouble faults.
   i) Connected devices shall be able to be independently power cycled.
   j) Live monitoring of status.
   k) Remote manual battery testing.
7. Manufacturer: Life Safety Power M-Class Unified Intelligent Power Supply.

2.5 MISCELLANEOUS EQUIPMENT

A. Local door alarm:

1. Power: 12 - 24 VAC/VDC @ 250 ma. max.

2. Door header combination devices.
    a) Kantech T-Rex #T.Rex-XL
3. Piezo only devices:
    a) Amseco P.A.L - 328
    b) Moose MPI47E

PART 3 - EXECUTION

3.1 GENERAL

A. Configure field panel communications as indicated on the Drawings.

B. Programming Requirements, Development, and Deliverables:

1. Produce fill-in-the-blank forms for the Owner to solicit user input for programming the system. The questionnaires shall identify each programming item that requires user input to configure the ACAMS and recommendations for the responses. These questionnaires shall be finalized in a series of meetings with the Owner's designated agent until such time that the questionnaires are completed, and the Owner has authorized the information to be input into the ACAMS.
2. The questionnaires shall include three series:
    a) The first shall be to the Owner's IT Department for network connectivity requirements.
    b) The second shall be dedicated to controller, alarm input and door programming, or hardware related programming and shall include:
        1) Controller naming schemes.
        2) Door and alarm input naming.
        3) Door unlock time and relock time.
        4) Door held open time.
        5) Door unlock and relock schedules.
    c) The third shall be devoted to alarm responses and related interface programming with associated action and reaction requirements to include:
        1) External alarm signaling requirements.
        2) Graphic map development and door and alarm display.
    d) The fourth shall be related to display of alarm messaging, map development and any requirements for alarm responses and reporting.
3. Upon completion, the programming questionnaires and associated programming database sheets shall be included in the operation and maintenance documentation.

C. Minimum Programming Requirements:

1. Program the alarm bypass or shunt time (the time the door can remain open before an alarm event is created) for 30 seconds, unless directed otherwise by the Owner's representative.
2. Program the door relock time (the time after which the door will relock unless opened) for 5 seconds, unless directed otherwise by the Owner's representative.
3. Program alarm response fields, door names, and any other user-defined fields with terminology and descriptions provided by the Owner.

4. Program access rights, password protection, system integration interfaces, holidays, area control, inputs and outputs, schedules, and elevator control.

D. Graphics:

1. Develop graphic maps that detail the facility and display inputs and outputs dynamically.
2. Maps shall be nested according to the following levels:
    a) Overall campus.
    b) Building.
    c) Floors.
    d) Further subdivided in alarm device location.
3. Utilize AutoCAD architectural floor plans that show walls, doors, windows, room names, and room numbers.

E. Control Panel Cybersecurity Configuration Requirements:

1. The following are minimum requirements:
    a) Place the access control system components on a private network, in a secured enclosure, and with updated firmware matching the existing installation.
    b) Enable HTTPS.
    c) Remove default user login, create a unique user account with a strong password.
    d) Add authorized IP Addresses.
    e) Disable web service, unless specifically required for operation.
    f) Disable discovery and SNMP services, unless specifically required for operation.
    g) Disable unused USB and SD interfaces.
    h) Enable AES or TLS encryption.
    i) Provide additional configuration changes per manufacturer's requirements.
2. Provide report manufacturer's certification that cybersecurity requirements have been met.

F. System Integration and Interfaces:

1. Upon an alarm condition or event to include but not limited to, an access point, duress button or other alarm input, intercom call, emergency phone call, the ACAMS shall cause the video surveillance system to:
    a) An alarm event message shall be transmitted to the associated workstations or consoles causing an audible and visual alarm signal.
    b) Where a local door sounder is adjacent to the door, it shall be activated until reset at the workstation or console.
    c) A graphical representation of the alarm scene (site or floor plan) with icons representing the open door, video camera, and other local devices shall be displayed on the graphical user interface (GUI). Icons representing active devices shall change color to indicate their state change (inactive to active).

3.2 MISCELLANEOUS EQUIPMENT

A. Fire/Life Safety Interface:

1. Locking devices controlling emergency exits connected to the building fire alarm system, if locked in the direction of egress, shall unlock upon initiation of an alarm signal at the building fire alarm control panel or upon loss of primary power to the building.
2. The use of battery or emergency power shall not be used to keep emergency exits locked in the direction of egress.

B. End-of-Line Supervision:

1. Provide end-of-line resistors to monitor 4-state supervision (cutline, short-circuit, switch open, and switch closed) at each intrusion detection input device.
2. Resistors shall be installed at the monitored device location, not at the control panel.
3. Provide pre-manufactured resistor packs, or devices with integral resistor networks.

3.3 FIELD QUALITY CONTROL

A. Tests and Inspections:

1. Program an access card to open all doors in the system. Program a second access card to open all doors in the system, but then classify the card as lost or stolen. Attempt to access each door using the valid card first, and the card classified as lost or stolen card second.
2. For access-controlled doors, test the following parameters or functions:
    a) A valid card read by an authorized user unlocks the door.
    b) A valid card read by an authorized user shunts or bypass doors forced alarm.
    c) Valid card read of a card reported lost or stolen creates an unauthorized use of lost card event in the system.
    d) A door forced open (or unlocked with a key) without the use of a valid card creates a “door forced” event and displays event on security workstation with operator instructions.
    e) Door held open beyond the door alarm shunt time creates a “door propped” event and displays event on security workstation with operator instructions.
    f) Where a local door sounder is located adjacent to the door, the event activates the sounder alarm until reset at the workstation or console.
    g) On the GUI, the event causes icons representing active devices to change color to indicate their state change (inactive to active).
    h) Door forced or door prop event automatically calls up the associated video camera image(s) (if any) on the designated video surveillance monitor(s).

B. Test Reports:

1. Print a report showing the valid card's activity during the test period as well as the alarm activity for the test period. Confirm that the report shows a valid access for each door in the system for the valid card, and that the card classified as lost or stolen generated an appropriate alarm or exception report for each door in the system. Present this report to the Owner.
2. Access control system functional test reports.

3.4 INSTRUCTION OF OPERATING PERSONNEL

A. System manufacturer certified trainers shall give operating and maintenance instructions on the access control system. Each session shall last at least 8 hours.

B. See Section 28 05 00, Common Work Results for Electronic Security for additional requirements.

END OF SECTION 28 10 00